THE THIRD REICH IS LISTENING

Inside German codebreaking 1939–45

CHRISTIAN JENNINGS

OSPREY

THE THIRD REICH IS LISTENING

Inside German codebreaking
1939–45

CHRISTIAN JENNINGS

OSPREY
PUBLISHING

Five people more than any made this book possible: my literary agent Andrew Lownie in London, my editor Kate Moore in Madrid and Oxford, my brothers Anthony in Rome and James in Yangon, and in Turin the indomitable Kat Sacco. Thanks must go to Italy, too. There can be few places more conducive to happy writing than Finale Ligure on the Mediterranean, or Bardonecchia in the Italian Alps.

CONTENTS

Preface

PART ONE: GERMANY ASCENDANT

1. Losing the Signals Intelligence Battle in World War I
2. The Enigma Salesman
3. Germany's New Codebreakers
4. Preparing for War
5. The Kriegsmarine Starts Listening

PART TWO: GERMANY OFFENSIVE

6. Two Navies at the Outbreak of War
7. Romanian Codes and Romanian Oil
8. Signals and Deception in the Invasion of Europe
9. Fighting the War in the Air
10. The Battle of the Atlantic
11. Classical Enemies, Modern Codebreaking

PART THREE: GERMANY AT WAR

12. Germany's Mediterranean Battles
13. Losing Enigma
14. The Good Colonel
15. Signals Intelligence and Cryptanalysis on the Russian Front
16. The Enigmatic Swiss
17. Rhubarb and Rodeo

18. U-91 and the Battle of the Atlantic

PART FOUR: GERMANY DEFENSIVE

19. The Battle of the Aegean
20. Insecure Enigma
21. The Coming Storm
22. Execution and Capture
23. The Collapse of the Third Reich
24. The Man with the Key has Gone

Epilogue: What Became of the Characters after the War?

Conclusion

Photographs

Chronology

Bibliography and Sourcing

Glossary

Endnotes

Acknowledgements

PREFACE

The Files

Spring 1945, Berlin and Bavaria

By late March 1945, the Red Army had stormed into Danzig in Poland, and crossed the border into Austria. In the west the Allies had captured Cologne and moved over the Rhine. With Germany under attack from all sides, the British and Americans then slowed their advance to allow the Russians to take Berlin. A month earlier in February, nearly a thousand American B-17 Flying Fortresses had attacked the Berlin railway network in the mistaken belief that the German Sixth Panzer Army was crossing the city by rail en route to the Eastern Front. Allied intelligence proved to be incorrect, but the dense bombing caused a firestorm that lasted for four days, and burned everything in its path to ash. Because the raid took place in daylight, and American General Carl Spaatz's aircraft used few incendiary bombs, the casualty toll was light for a major raid. A total of 3,000 people died, 20,000 were wounded and 120,000 were made homeless. But it made the German capital an increasingly difficult and highly dangerous location in which to work.

The cipher bureau* of the Wehrmacht High Command, called OKW-Chiffrierabteilung, or OKW-Chi for short, had in fact long departed Berlin. In the winter of 1943–44 aerial bombing had made it impossible to stay in the capital any longer. By the time the cryptanalysts left some of them had already been working in a series of deep cellars in a residential part of the city.

There was no central heating, the doors had in some cases been removed for firewood, and in the rooms where the cryptographers worked a layer of white plaster dust covered everything, brought down by the repeated shocks of aerial bombing on the buildings above them. In that cold winter, some of the men and women worked wearing gloves or mittens against the cold, making it even harder to try to write signals decryption reports, in pencil, by flickering electric light and candles. At that point in the war, as 1943 turned into 1944, the British and American signals that OKW-Chi's cryptanalysts were decoding were filled with details of the Allies' steady northern advance up through Italy, their plans for a second front, and the Red Army's encirclement of the Germans at Korsun–Cherkassy. There were also decrypted reports about Allied air raids on Germany, becoming ever more frequent, as well as the glaring failure of Admiral Dönitz's U-boats to prevent Allied supply convoys, sometimes hundreds of ships strong, sailing across the Atlantic. While not imminent, the end of the Third Reich could be smelled in the air. But even so, Germany's codebreakers were still hard at work monitoring, intercepting, decoding and reading signals from agents, armies, aircraft and ships from different countries.

OKW-Chi was only one of the ten German signals intelligence agencies, but by July 1944, just after the invasion of Europe, it was working on cracking codes from enemy forces and neutral governments as well as foreign agents in forty-one different European and non-European countries. By March 1945, as the American bombers continued to pound Berlin, the agency was working from the Wehrmacht signals school at Halle, in the central part of eastern Germany. Wilhelm Fenner was the cryptographer and administrator in charge of the OKW-Chi codebreaking department, and by the end of that month, he decided that they had to evacuate and head south to Bavaria. So hundreds of kilograms of secret documents were loaded into wooden packing cases that had once contained radio interception equipment. A company of soldiers found trucks and petrol, and the staff emerged from underground into the grey, half-daylight of the city. Some of the staff were ordered to head for the railway. Others boarded the lorries, and only when they pulled out of Halle's southern suburbs did the air begin to clear. None of the cryptanalysts and signals intelligence people on the trucks knew much about where they were going, or what would happen to them. They sat in the back of bumping lorries for hour after hour, the space between them and their colleagues opposite filled with the big, wooden cases. These were loaded

with some of the most important intercept and decoding reports and files that OKW-Chi had worked on since 1938. Their superiors were determined that none of this would fall into the hands of the advancing British, Americans or Russians. And among the men and women on the lorries that day, both soldiers and civilians, there was a silent, urgent, mutual understanding that nobody, but nobody could be allowed to fall into the hands of the Red Army.

OKW-Chi burned all non-essential material, but that which was deemed too important to be destroyed was taken from the headquarters at Halle towards a lake in southern Bavaria. The meandering journey of the OKW-Chi team took nearly ten days. As they headed further south, so the weather got cautiously warmer. It was full spring by the time they arrived in Bavaria. By lorry and train, they moved southwards towards Nuremberg, Munich and Berchtesgaden, where Hitler had his 'Eagle's Nest'. Outside the town of Rosenheim, fifteen miles south of Munich, the convoy pulled off towards the mountains that loom on the Bavarian and Austrian border. By the beginning of the second week in April, the soldiers and civilians of OKW-Chi had billeted themselves in a series of deserted schools, hotels and railway buildings in a small Alpine town called Schliersee. It was set around a beautiful blue lake. One morning they saw SS men from an artillery unit dumping wagon loads of mortar and artillery shells into the water, and burning their paper files on the shore. The day after that some of the men from OKW-Chi and a few soldiers put the boxes full of their own secret files onto two railway wagons: these were shunted up the sidings by the lake's edge, and from it the men hurled dozens of boxes into the muddy water. Another group loaded boxes and pieces of technical equipment onto a raft, rowed out into the lake, and dumped the material into the water. The German soldiers and civilians then moved off towards Munich again: there were orders to join a combined army and air force unit that was being put together across Bavaria, made up of stragglers of all ranks and units. This would then surrender in an organized manner to the Allies, who were fast approaching from the west. Meanwhile the crates containing OKW-Chi's records lay thirty feet down in the soft brown mud of a Bavarian lake, settling gently onto a layer of SS artillery shells.

•••

In July 1944 the British and Americans decided to try to capture the scientific

secrets of the Third Reich. The Allies were anxious to know what kind of technological advantages the Germans had achieved over them. How far advanced were they when it came to guided rockets, precision bombs, jet aircraft and main battle tanks? And which codes, from both Allied and neutral countries, had they broken? How? When? Using what equipment or inside information? In short, what was there in terms of technology and intelligence that the Germans had that the Allies didn't?

By the autumn of 1944 it was clear the Allies were soon going to win the war. So they formed four teams of intelligence 'hunters' who would comb Germany and Austria and the Low Countries as the war lurched towards its inevitable conclusion. The Combined Intelligence Objectives Subcommittee gave codenames to these operations: ALSOS would search for nuclear information and research, OVERCAST would try to capture anything to do with V1 and V2 rockets, and SURGEON would cover the hunt for avionics and jet technology. Of all four intelligence hunts, the one that was kept the most secret was called TICOM. In its sights was anything to do with the signals intelligence agencies of the Third Reich.

TICOM, or the Target Intelligence Committee, had three aims: to discover what inroads the Germans had made, and how, into breaking Allied naval, military, air force and diplomatic codes; to try to capture precious signals intelligence personnel, records and equipment before the Russians did; and to finally work out the level of German intelligence cooperation with the Japanese, whose country the Allies were then planning to invade. Drawn from teams of British and American naval, army and air force officers who had received training at Bletchley Park, the TICOM teams would go into the Third Reich alongside, or just behind, the front-line troops. One early deployment plan was to parachute the teams into Berlin with the 101st Airborne Division, let them search the destroyed capital of the Reich for intelligence information, if necessary fight against any die-hard elements of the German SS who got in their way, and then wait for American and Russian armoured columns to break through to relieve them. The scholarly TICOM officers had put on their uniform knowing they could easily be sent into armed action against a German or Japanese or Italian enemy. But the idea of a parachute drop into the dying days of the embattled Berlin defensive cauldron was something they were happy to see cancelled.

Instead, they would drive into occupied Germany. It would still be extremely risky. Even after the formal surrender, German forces would still be

armed and some could be looking for last stands. The TICOM officers were all 'Ultra Cleared', and knew the full secrets of the breaking of the Enigma codes, so even at this late stage of the war could not be taken prisoner. As a result a unit of British Royal Marines was assigned to protect them, an outfit almost as idiosyncratic and individual as themselves.

30 Assault Unit (AU), Royal Marines, was the brainchild of the maverick and flamboyant naval intelligence officer, Lieutenant Commander Ian Fleming. Before the disastrous British and Canadian raid on the French port of Dieppe in August 1942, Fleming saw that there was the potential for a commando unit that would go into action alongside conventional forces, and under cover of battle steal or kidnap intelligence documents, machinery or personnel. Based on the coast of West Sussex in the town of Littlehampton, 30 AU, as they were known, were camouflaged as part of a larger Royal Marines commando unit. At Dieppe, their mission was to fight their way to the German headquarters in the centre of the town and steal a naval Enigma machine. Operation *Jubilee*, the assault on Dieppe, however, was a notable disaster, and the Marines of 30 AU – who included a safe-cracker in their ranks – didn't even make it off their landing craft, so heavy was the German incoming fire on the beaches where they were meant to go ashore. Three years later, however, the unit was ready to go into Germany with the TICOM teams.

By 1 May, Hitler was dead, and the Red Army had taken Berlin. By now divided into six separate teams, the TICOM officers went into the chaos of a Germany where six years of war had stopped only hours before. Their reports and documentation from those first days are filled with a mixture of cliff-edge, trigger-finger tension, and moments of the theatrical lunacy and explosive human spirit often found in wars. Half of the German civilian population hated them and the other half welcomed them with open arms. The roads they drove were sometimes filled with thousands of displaced persons from Russia and France and Germany, prisoners-of-war (POWs) just released, soldiers and refugees, in a country where violence, desperation and death hung in the air like apples that any moment could fall from the tree. At other times there were moments of peace and calm in the midst of what one TICOM officer called 'our private war'.

They stayed in private houses, in the tented barracks of US Army units, in deserted holiday hotels where the staff had fled only hours before, and the visitors' books were sometimes filled with the names of senior Nazi officials.

They camped out under the stars of the German spring, and in Bavaria they combed through cellars and barracks, just recently deserted by fleeing German troops. They followed up every piece of passing rumour and information they could glean from anybody who had it, about where Germany's codemakers and codebreakers might have fled. Their search took them through the shuddering heartland of a surrendering country and a dying war, set against the glorious spring canvas of the first days of peace. Outside Munich they found two tons of maps and caches of fused stick-grenades in one house, they searched a signals dump in a lunatic asylum and by the roads they saw half-burned SS uniforms. They scoured an empty summer house belonging to Von Ribbentrop, and questioned a wandering SS man who said he might know something about invisible inks. Another rumour told them that high up near a mountain lake was a secret research station where the Nazis decrypted signals. On their way up this mountain they found a troop of American soldiers making themselves comfortable in Himmler's hunting lodge, six French Nazis pretending to be road workers in one Alpine hut, and further up the slope a ski chalet where four ex-Luftwaffe men and three women were enjoying themselves, but no secret research station.

Meanwhile, in the lobby of the Hotel Astoria at Bad Gastein near Berchtesgaden, 126 Japanese diplomats, led by their Berlin ambassador Baron Oshima, waited silently. The Japanese ambassador had been a close confidant of Hitler's, and the Americans, who had broken the Japanese diplomatic cipher, which they codenamed 'Purple', had been reading his communications with Tokyo. The material he produced was highly authoritative – among the nearly 1,500 transmitted reports was one from 6 June 1941, where Oshima told his superiors in Tokyo that Germany would invade the Soviet Union on 22 June. In mid-April 1945, he had met with the German foreign minister Joachim von Ribbentrop, and vowed to remain in Berlin to the end, alongside Hitler and his advisers, but a personal order from the Führer ordered him and other diplomats to leave Berlin. So he travelled to Bad Gastein to join his wife; the Americans subsequently arrested them, and transported them to the United States by ship.

Meanwhile a British TICOM officer accompanied the Royal Marines of 30 Assault Unit to the small island of Mainau, which sits off the shore of Lake Constance on the Swiss–German border. He was following a tip-off that the Germans had evacuated an experimental research station there, bringing

scientists who had been working on V2 rocket technology from the Baltic coast at Peenemünde. At 1,000 metres long by only 600 at its widest point, Mainau is a huge arboretum containing some 500 types of trees, as well as hundreds of different varieties of roses, dahlias, azaleas and rhododendrons. At the entrance to the bridge linking the island to the mainland, a sentry said that the TICOM team couldn't go any further, since the island was private property and neutral territory, belonging to Prince Bernadotte of Sweden. The French, however, seemed to be using it as a displaced persons camp. The French medical officer told the British Marines and the TICOM officer that there was no point in their inspecting the island as two of their colleagues from British military intelligence had already done so. But, he said, should they wish to have a look themselves, they'd need clearance passes from local authorities in Konstanz. The Marines turned their jeeps around and returned to the town, only to discover that every single public office was closed for the day in honour of a state visit by the sultan of Morocco. It was yet another frustrating dead-end. Indeed, by the last week in May, there had been no real breakthroughs for the investigators, and it seemed they had simply been chasing rumours and misinformation for weeks. On the 31st, for instance, it just rained and rained all day, and one of the TICOM teams reported that they simply stayed indoors in the deserted Bavarian house they had occupied, and drank wine from a cellar they had discovered in the town of Kaufbeuren.

But then they got lucky. A party of senior Wehrmacht and Kriegsmarine officers, on their way to surrender to the Allies at Rheims, met another of the TICOM teams operating further north. One of the German army officers in the group was a Lieutenant Colonel Mettig, who had been the second-in-command of OKW-Chi the year before. The war was over, he said, and nobody had anything more to hide. The Americans were now the Germans' allies, and both sides should work together against the Russians. Go to Bavaria, he said, and find the lake called the Schliersee.

When the British and American officers arrived in the town two days later at the end of June, the first person who offered to help them was a small, neat man who had been a policeman in Vienna. He wore civilian clothes and the armband of the Freiheitsaktion Bayern, a local anti-Nazi militia that had the backing of the Allied Military Government in Munich. 'Come with me,' he said. 'I'll show you where the SS and Wehrmacht were.' The teams searched three hospitals filled with wounded soldiers, and a local school, and found there was nothing in the post office or the local hotel: bathing huts lined

along the lake shore hid little but empty boxes stamped with the Wehrmacht eagle. In the town railway yard were two Luftwaffe railway wagons full of photo reconnaissance equipment, the trucks damaged and looted after Russian displaced civilians had broken into them to take refuge from the winter. Accompanied by their militia guide, the Allied teams found some civilians who told them that two days before the Germans fled, they filled two railway cars with boxes of papers and threw them into the lake: the information seemed to be correct, for in the muddy gravel at the edge of the water the TICOM officers found some half-burned SS personnel papers, and pieces of teleprinter machinery. One British and one American officer then took a boat and made an initial attempt to search the bed of the lake just beyond the shore; several times their ropes snagged on something very heavy, which they could not drag to the surface.

Then they had another breakthrough. In late July, American soldiers from the US Third Army started dragging the lake for the body of a soldier who had drowned while swimming; they found a large box, which they hauled to the surface. It was full of documents describing the operations of OKW-Chi. The American army then called in both TICOM and a unit of specialist salvage engineers based in Le Havre, on the French Atlantic coast, where they maintained the pontoons of the artificial harbours that the Allies still used to land troops and supplies. At the end of August the Americans drove across France and down through Germany, bringing four divers with them, and built a large raft with an engine and a crane on it, which they then used to search the bed of the lake. It didn't take them very long to find twenty-eight large boxes, lying in thirty to fifty feet of water, surrounded by SS artillery and mortar shells. It was a significant part of the OKW-Chi archives.

TICOM teams working in northern Germany eventually had similar successes: they occupied the intercept station at Neumünster on the German–Danish border, and the signals school at Flensburg-Mürwik, where the German naval signals intelligence agency had its headquarters at the end of the war. They captured the details of '*Flusslauf*', or 'Running River', a new naval cipher that was due to go into effect on 5 May, meaning that the Allies would not have been able to continue to read Ultra signals in the last vital days of the war. By the end of September, the TICOM teams had found, captured and started interrogating German personnel from navy, army, air force and Foreign Office cryptanalytical units. These interviews took place in Bavaria, Austria, Britain and in central and northern Germany. Eventually

they would stretch to tens of thousands of pages, and to them would be added all the signals codebooks, teleprinter machines, maps and assorted documents that the Allied search teams were to find between then and late summer 1946. This huge amount of material became known in American and British intelligence circles as the TICOM archives.

The war ended. Codebreaking operations at Bletchley Park wound down, as the British and Americans were suddenly facing a new enemy: Russia. The Cold War began, and several of the German cryptanalysts who had led signals intelligence agencies during the war went on to work for the Americans, or the new German government. The huge TICOM archives were stored in depositories in Britain and the United States. And there they stayed as the 1940s turned into the 1950s. Both Britain and America consulted them from time to time, as in 1952, when the US Navy decided to carry out a definitive analysis of the Battle of the Atlantic and the part played in it by German decryption of Allied naval codes, and British codebreaking efforts at Bletchley Park. In 1968 the British turned to it again, after the Germans 'discovered' nearly 100 pages of London's confidential wartime diplomatic telegrams in a foreign ministry archive in Bonn. How had they got there? Whitehall wanted to know. The Germans hadn't been breaking British Foreign Office codes as well as their naval ones, had they? Similarly, what on earth were hundreds of decoded British naval signals from the Mediterranean, from 1940 to 1943, doing sitting on shelves in a naval archive in Rome? Had the Italians been breaking British codes too?

And then in the early 1970s, all this was eclipsed when the British and Americans declassified the files of the Allied wartime codebreaking operations at the Government Code and Cypher School. Enigma, Ultra and Bletchley Park became history. Forty years of books and films resulted.

The TICOM archive slumbered on, as did all the myriad documents and maps and diaries and machines and codebooks that the Germans had left behind in the signals outposts of their wartime empire, from Croatia to Italy, from Russia, Romania and the Ukraine to Estonia, and from Prague to Paris. As the internet grew in the year 2000, Britain and America started declassifying the TICOM archives, either returning the material to Germany, or keeping select items in their own museums and public archives. The daily wartime operational diary of German U-boat headquarters, for instance, stayed well put in a naval museum in Maryland. A very small handful of keen bloggers and authors documented the trickle into the public domain of new

material about German codebreaking in the war, but not surprisingly, none of it had a twentieth of the impact that the disclosure of the Enigma and Ultra secrets did.[†]

•••

Autumn 2017

The first snows fall late in the Alpine resort of Bardonecchia, the most westerly town in Italy. By the first weekend of November, the endless blue skies and bright sun that have been the currency of the weather since April have started to fade. The leaves on the chestnut trees that line the town's streets have begun to fall. A brisk wind says firmly that winter is on its way, and on Remembrance Sunday, 5 November, the peaks above the town are covered in white. On the grey stone memorial in the Vittorio Veneto Remembrance garden, there are forty bronze plaques to the inhabitants of the town who died in World War II. They represent a cross-section of all the places where Italian soldiers went to fight and die in the war, either on the side of the Germans, or, as partisans, against them. They are also a reminder of the massive geographical and political span of the fighting – Bardonecchia is a small Alpine town, and these are but forty names, but they stand to bear witness to a tiny fraction of the war's vast cost and reach. There's Private Luigino Bompard, thirty-one years old when he was killed in Sarajevo, and Private Attilio Garnier who disappeared in Croatia. Staff Sergeant Sergio Tarraboiro went down on a ship off Malta in 1942, and Alpine Trooper Alberto Vallory died on the Russian Front in 1942. Partisan Giuseppe dalla Vecchia died in Bardonecchia itself in 1944, aged only sixteen, and Alberto Mallen was deported to Mauthausen concentration camp. A children's playground, which sits quietly under the pine trees by the ski slopes, is now named after him.

Sometime after midday on Remembrance Sunday, somebody arrives with a gas canister, which is attached to a metal device representing the eternal flame, and lit. Its small blue flames flap and roar in the cold wind while the memorial garden waits for the arrival of local officials. Thirty minutes later it's over, and the sole guardian of the garden is a large wreath of bay leaves, half the height of a man, that leans against the memorial stone. Snow clouds scud sideways across the mountains opposite, while the winter is not the only

thing to have arrived on that cold afternoon. Inside, out of the wind and away from the snow, there is an email waiting. It is from the political archives of the German Ministry of Foreign Affairs in Berlin; with characteristic efficiency they are sending over their new Excel spreadsheet. It details 3,917 items. Navy codebooks from France in the 1920s, maps of Bulgaria, lists of Spanish military ciphers, Chinese, Yugoslav and Italian diplomatic codes, papers showing Russian bigram ciphers, the 1941 Romanian army codebook, Ethiopian diplomatic codes from 1944, Japanese and Belgian foreign ministry ciphers. The list goes on and on. These are all items that the TICOM teams eventually found in 1945 and 1946 in Germany, and took back to England. They lay in British national archives for fifty-five years, and were returned to Germany only in 2000. And given that other museums and archives across Europe, and in America, also contain other large parts of the TICOM archive, it gives an insight into the breadth and ambition of the Third Reich's codemaking and codebreaking successes, and failures. As to what the Germans were, or weren't, able to achieve with all or some of these cryptanalytic acquisitions? This book touches the tip of a very large iceberg, and attempts to provide just a few of the answers.

---

* In this book the spelling 'cipher' is used. When time-specific spellings or quotes are used, as in the Royal Navy's 1930s and 1940s use of 'Cypher', this is put into the text.

† A chronology of events in this book from 1914 to 1945 is included here.

PART ONE

GERMANY ASCENDANT

Chapter One

LOSING THE SIGNALS INTELLIGENCE BATTLE IN WORLD WAR I

On Saturday 2 August 1914, the German light cruiser SMS *Magdeburg* was steaming through the Gulf of Finland. Its destination was the port of Libau, on the Latvian coast. With it sailed another cruiser, the *Augsburg*, as well as a destroyer and a minelayer. Germany had declared war on the Russian Empire the day before, and the four ships had orders to lay mines outside the Libau harbour, and then bombard the port in preparation for a German infantry attack. And so the first shots that Imperial Germany fired against the forces of Czar Nicholas II came as the *Magdeburg* shelled Libau with its 4.5-inch guns. The Russian garrison of the city fled. The *Magdeburg* stayed in position offshore, firing on other targets. A minefield was laid by the *Augsburg*, though it was so poorly marked that it proved more of a hindrance to the Germans than to their enemies. For the next three weeks, the two vessels patrolled the Gulf of Finland, accompanied by destroyers.

On 26 August, the German ships were sailing in heavy fog when they lost visual contact with each other. The fog was thick enough that signals lamps could not cut through the thick white gloom. The first that the crew of the *Magdeburg* knew that they had sailed off course was when a thunderous crunch rocked their ship. They had run aground. They were stuck fast on rocks, on the small island of Odensholm just off the coast of the Russian province of Estonia.

One of the destroyers with them heard the sound of the *Magdeburg* hitting the underwater reef. The fog started to lift. The destroyer attached a line and tried to tow it off, but the *Magdeburg* was hard aground. Its captain gave orders to destroy the ship, and then abandon it. Three things then happened simultaneously, and very fast. A wind started to clear the fog, and out of it appeared two Russian cruisers. They opened fire. Then the demolition charges the German sailors had placed in the forward compartments of the *Magdeburg* detonated prematurely. Fifteen of the crew were killed. Most of the remainder boarded the destroyer sent to assist them. With the forward sections of the cruiser now on fire, the captain did not have time to throw all of the ships' secret papers overboard. Or to make sure they were taken on board the destroyer.

Like many ships in the Kaiserliche Marine, the Imperial German Navy, the *Magdeburg* carried a small, lead-lined chest for use in such emergencies. The captain put the ship's log, maritime charts and two copies of a secret signals codebook into the chest and threw it overboard into the shallow, clear waters of the Baltic. The Russian cruisers were now closing in fast. The forward sections of the *Magdeburg* were blazing. The captain set fire to a third copy of the signals book. The fog continued to lift. The German destroyer moved off as fast as it could, leaving the captain and fifty-seven of the crew members still on board, along with a fourth copy of the Imperial German Navy's *Signalbuch der Kaiserlichen Marine*, the SKM codebook, still in the safe in the captain's cabin.

The codebook was still there as the Russians boarded the ship and took the captain and the other sailors prisoner. They decided to leave the *Magdeburg* where it was, and then scrap it. A Russian diver was sent over the side. He recovered the chest containing some of the ship's papers and the two codebooks. The captain's cabin was searched and the fourth copy of the signals book found. They were immediately taken on board one of the Russian cruisers. The Russians then contacted the British naval attaché in Petrograd, as St Petersburg had just been renamed. The deal was simple. They offered their allies in the Royal Navy a copy of the prized SKM codebook, on the condition that a British ship came to collect it. As a result, the Admiralty gave orders to the cruiser HMS *Theseus* to sail from Scapa Flow; it arrived on 7 September near Murmansk. It successfully sailed back to Scotland, docking on 10 October, with two senior Russian naval officers on board, and copy no. 151 of the SKM codebook. By 13 October, the book

was in London. Winston Churchill was then First Lord of the Admiralty. He was overjoyed. He gave an enthusiastic account of the incident, when he described receiving these 'sea-stained priceless documents' from Britain's Russian allies.*

> At the beginning of September 1914, the German light cruiser SMS *Magdeburg* was wrecked in the Baltic. The body of a drowned German under-officer was picked up by the Russians a few hours later, and clasped in his bosom by arms rigid in death, were the cipher and signal books of the German Navy and the minutely squared maps of the North Sea and the Heligoland Bight. On 6th September the Russian Naval Attache came to see me. He had received a message from Petrograd telling him what happened, and that the Russian Admiralty with the aid of the cipher and signal books had been able to decode portions at least of the German Naval Messages. The Russians felt as a leading naval Power, the British Admiralty ought to have these books and charts.[1]

It was just over two months into World War I, and on the battle front called signals intelligence, the German navy was already on the defensive. Then within days of the boarding of the *Magdeburg*, it happened again. On the other side of the world the Germans lost another of their vital signals codebooks. On 11 August, a boarding party from the Royal Australian Navy approached a freighter sailing off Port Phillip Heads, due east of Melbourne. The SS *Hobart* was joint-owned by a German and an Australian steamship company, and had a German crew. News that war had broken out had not reached the ship. So the Australian naval party simply pretended to be a quarantine inspection team. The *Hobart*'s officers allowed them to circulate around the ship, supposedly checking for any signs of yellow fever among the crew. At midnight, one of the Australian sailors noticed the German captain of the *Hobart* try to throw something overboard. It was the ship's papers and a large codebook: the *Handelsverkehrsbuch*, or HVB codebook, which every German merchant ship carried. The book contained the codes for the signals which the German merchant fleet used to communicate with their navy, and with coastal stations. Not every German merchant ship had a copy – it was restricted to the eighteen largest German steamship companies whose ships were equipped with wireless. Capture of the HVB codebook meant that any party who could decipher the Merchant Navy codes could potentially read

the signals of the Imperial German Navy. It was originally issued in 1913 to all warships with wireless, to naval commands and coastal stations. The code used thousands of four-letter groups to represent different words. The book was copied and sent to London, where it arrived in the second half of October 1914. German intelligence were aware in November 1914 that the HVB codebook had fallen into enemy hands, as evidenced by wireless messages sent out warning that the code was compromised, but it was not replaced until 1916.

Lightning then struck the Germans a third time. In the second week of October 1914, the Royal Navy and the German fleet were skirmishing in the northern reaches of the English Channel. The Battle of the Yser was fought for control of the coastal towns of Dixmude and Dunkirk. The British navy were bombarding German positions from the sea; German destroyers then attacked them. On 17 October Captain Cecil Fox was commanding a task force made up of the light cruiser HMS *Undaunted*, and four destroyers, HMS *Lance*, *Legion*, *Lennox* and *Loyal*. He sailed to meet a German attack, and ran straight into four German destroyers, *S115*, *S117*, *S118*, and *S119.* They were sailing down the Channel with orders to lay mines. The Royal Navy ships took less than an hour to sink the German vessels, after which the captain of *S119* threw overboard all his secret papers in a lead-lined chest. On 30 November a British trawler dragged up the chest in one of its fishing nets. It contained a copy of the *Verkehrsbuch*, or VB codebook, normally used by flag officers of the German navy.

The code consisted of 100,000 groups of five-digit numbers, each with a particular meaning. It had been intended for use in cables sent overseas to warships and naval attachés, embassies and consulates. It was used by senior naval officers with an alternative *Lambda* key, but what it was doing on a small destroyer at the start of the war remained a mystery. Its greatest importance during the war was that it allowed access to communications between German naval attachés in Berlin, Madrid, Washington, Buenos Aires, Peking and Constantinople. This codebook was even more important than the two captured off Australia and in the Baltic.

British Naval Intelligence Deciphers German Naval Codes

British codebreaking and signals intercepts operations were in their infancy in 1914. This was to be expected, as the electronic medium they were trying to

break into, wireless telegraphy, was also new. Guglielmo Marconi had perfected his invention only in 1907. In 1912, the high-power radiotelegraph transmitter installed on the *Titanic* for sending passenger 'Marconigrams' and for operational use was considered the height of technical innovation.

At the Old Admiralty Building in London was a large room with the designated number '40'. This was the headquarters of the Royal Navy's nascent codebreaking unit; for the rest of the war it was simply called 'Room 40'. There was no shortage of wireless signals to work on. Three years earlier, in 1911, the British Imperial Defence Committee had made a far-sighted decision; German undersea wireless cables would be cut in the event of war breaking out. This, reckoned the committee, would force the Germans to send messages either by wireless networks owned by other countries, or in code on wireless networks not dependent on cables. In both cases, if the British could capture the codebooks, or crack the ciphers, the information would be accessible to them. They were proved right. Three days after war with Germany was declared on 4 August, the British cut five of Germany's trans-Atlantic cables which ran down the English Channel. Coded German wireless traffic promptly increased. And as each message was encoded using either the SKM, VB or HVB codebook, this gave the British intelligence officers and civilian staff a huge amount of material to work on. Room 40 reportedly referred to the capture of the three German codebooks as the 'miraculous draught of fishes'. At the outset, the interceptors used Post Office wireless intercept equipment, and technology from Marconi and from private radio enthusiasts. But when the captured German books first arrived at the Admiralty's Intelligence Division at Room 40, none of the naval officers were able to decipher them.

Simply put, nobody there was sufficiently versed in the technicalities of codebreaking. As such, the first director of the division, Admiral Henry Oliver, started recruiting hard. He had been in charge of the Royal Navy's navigation school and also had an unorthodox operational approach. At the beginning of the war in September 1914, he had been sent to Antwerp to work with allies from the Belgian naval intelligence division and civilian staff from the Antwerp Port Authority. There were thirty-eight stranded German merchant ships in the harbour, impounded under wartime restrictions. Oliver and the Belgians went on board these ships, and simply blew up the engine-rooms of all of them.

First and foremost in his mind was the need for strict confidentiality. He

decided to focus on two groups of potential recruits for his new codebreaking and signals intelligence department, both deemed trustworthy. These were naval officers and cadets from the Royal Navy's colleges at Dartmouth and Osborne, and Oxbridge men who had studied German, Maths and Classics (the study of ancient Greek, Latin, Ancient History and Philosophy). Oliver was succeeded shortly afterwards in the position of director by Admiral Sir William Reginald Hall, nicknamed 'Blinker', so-called because of a facial twitch that reputedly caused his face to flash like a naval signals lamp. Among those who arrived to lead and to staff Room 40 were the director of naval education, Alfred Ewing, who listed cryptology as a hobby; Nigel de Grey, a fluent French and German speaker who had been working at Heinemann publishers; and William Montgomery, a Presbyterian minister who had translated theological books from German.

The SKM codebook, when it arrived, was given to a German speaker who had just been recruited to work in the naval intelligence division, a Royal Navy paymaster named Captain Charles Rotter. He was one of the few men working at the Admiralty who knew anything about ciphers and encoding: a crossword enthusiast and mathematician, he quickly recognized that the signals from the SKM codebook were being encoded using a substitution table. He knew the principle of this was simple. Each letter of the alphabet was replaced by another. A 'key' told the user which letter of the alphabet to substitute for which. So if, for instance, the substitution for the letter H was N, it followed that I became O, J became P, and so it thus continued alphabetically. The astute naval paymaster applied what is known in cryptology as Kerckhoffs' Principle: to assume that everything about a given code or system is already known, apart from the key. It was named after a 19th-century Dutch cryptographer, Auguste Kerckhoffs.[†]

Rotter knew that if the same substitution table was used for long enough, it could easily be broken by frequency analysis. E is the most common letter in English, followed by T, then A, I, N and so on. If a coded message using a simple substitution table contains the letter K, for example, more than any other, there is a strong chance that K must correspond to E. The three most common letters in the German language are E, N and I. So if three letters – say, G, W and C – repeat frequently through a message, there is a strong chance they correspond to E, N and I. To protect a code, therefore, the same substitution table must not be used for long enough to make it vulnerable to frequency analysis.

The SKM book captured from the *Magdeburg* was similar to the signals books then used by any large navy. It had 34,300 separate instructions, almost all of which were pre-determined instructions used by naval ships – '*I am opening fire, I am making smoke, I am entering harbour on the port side, my position is as follows*'. Each of these thousands of instructions was represented by a different group of three letters. The signals also used four extra letters, alpha, beta, gamma and rho, taken from the Greek alphabet. This would have made transmission by Morse code impossible as the extra letters did not appear in the classical, 26-letter Morse alphabet. As such a separate substitution table was attached to the SKM codebook to identify and spell out individual letters such as alpha or gamma. Using the available intercepted signals, the captured German codebooks, and his knowledge of substitution tables, Rotter got to work. British wireless listening stations on the North Sea coast had by now started picking up German naval messages every day. With the help of the SKM book it did not take him long to start transcribing some of these into plain, German text. It occurred to him that the messages were not as simple as they appeared: they had also been encrypted before being sent. Rotter needed a numerical or alphabetical key to break this additional encipherment.

The SKM was a signal book, as had been used by navies all over the world for hundreds of years. The most famous example of the signal book's use is perhaps Nelson's signal at Trafalgar: '*England expects that every man will do his duty*.' Each of the different signal flags used by HMS *Victory* represented a number, and used in threes they made up three-figure numbers that related to different words in a codebook. The signal book assigned three-figure codes to single words, so that 'England' became 253, 'expects' became 269, 'that' became 863 and so on. Words not in the codebook, like 'duty', had to be spelled out, using a simple alphabetic substitution table: D became 4, U 21, T 19 and Y 24. (Nelson originally wished to say 'England confides' rather than 'expects', but since 'confides' was not in the signal book, 'expects' was used to save time.)

The SKM codebook was a more elaborate version of this system, assigning four-letter codes to a large number of commonly used words and phrases. It also contained a substitution table whereby any expressions not included in the codebook could be spelled out letter by letter. The problem was that the intercepted messages that Room 40 was working on could not be read with the codebook alone, for it was encrypted with a further monoalphabetic

substitution.

Alphabetic substitution tables are of two types: monoalphabetic and polyalphabetic. The former is the easier to crack, as it uses only a single set of substitutions: in other words, one letter of the alphabet is substituted for another. As soon as enough encrypted messages are available, a monoalphabetic code can be broken with straightforward frequency analysis – by determining which coded letter obviously corresponds to 'E', which to 'N', which to 'I' and so on. Sometimes, to prevent this, more sophisticated codes use a series of substitution tables, jumping from one to another at given intervals in the message. This is the principle of polyalphabetic substitution. Once Rotter recognized that the plain text (i.e. unencrypted text) had been encoded via the SKM codebook, and then further encrypted only by a monoalphabetic substitution, his task became simpler. Since the underlying text was not plain German but the four-letter groups of the signals codebook, frequency analysis based on the occurrence of letters in German was of no help. Nevertheless, the problem was a fairly simple one. It was possible to identify frequently occurring groups in the encrypted German messages the British were intercepting, and guess at their meanings. The same patterns of consonant-vowel-consonant could be identified, both in the codebook and in the encrypted messages, for the Germans wanted their code groups to be easily pronounceable. Working all of this out from scratch, it took Rotter three weeks to reconstruct the monoalphabetic substitution table that provided the key to the SKM codebook.

The German transmitting station at Norddeich, on the German North Sea coast, provided definitive proof of this 'key'. They had sent a series of messages earlier in October 1914 detailing the movement of a flotilla of destroyers approaching the Dutch coast. The messages were numerically sequential and repeated themselves, with the same words and numbers used at the beginning of each message: '*S116, S107, S139 heading towards Zuiderzee, position as follows …*' the only variant being the position itself. So once the first message was deciphered, the others followed. It turned out, as Rotter had estimated, that the Germans were using a substitution table for encipherment. This was a huge benefit for him, as it provided verified access into the Germans' signals. It also meant better working conditions, as the director of British naval intelligence was so concerned about secrecy that the paymaster was confined to working in a room all by himself. Only after cracking the decryption substitution table in November 1914 was he allowed to rejoin his

colleagues. In his absence, they had begun trying to make sense of the German HVB codebook. And should the British have needed any more German signals material, or captured codebooks, then 1915 brought them another surprise.

British troops captured, and then impounded, the luggage and equipment of a German explorer and secret agent in Persia called William Wassmuss. The bags were sent to London unopened, and Admiral 'Blinker' Hall discovered that they contained a copy of the German diplomatic codebook. Another source of captured codebooks then came from German U-boats that had been sunk by the British. Royal Navy divers from the Admiralty's salvage section would be directed to the recently sunken boats, often working in harrowing circumstances among the drowned German crews. Shipwright E.C. 'Dusty' Miller was one Royal Navy salvage expert. He described diving on a U-boat in the Channel. He entered through a hole blown in the submarine's hull, bumping against floating corpses, and found naval codebooks in a metal box in a small compartment aft of the officers' quarters. Working conditions were testing. 'The dogfish are about and will eat anything,' he wrote:

> In the mating season they naturally resent any intruder, and on lots of occasions when they chased me I offered them my boot, and they never failed to snap at it … there were some pretty weird scenes inside the boats … I found scores of conger eels, some of them seven to eight feet long, and five inches thick, all busily feeding … they gave one a bit of a shock.[2]

The British Gain the Upper Hand in the Signals War

'Their (the Germans') folly was greater than our stupidity,' commented Alastair Denniston, one of the senior staff members of Room 40, on the Germans' operational approach to their signals intelligence, and Britain's technical shortcomings.[3], ‡ Naval warfare between Britain and Germany in 1914 and 1915 was centred on three priorities. The first was the tactics of blockade, of trying to keep each other's fleets confined to home bases such Kiel, Bremen, Portsmouth or Scapa Flow. The British had blockaded Germany and were preventing German naval vessels from gaining access to the Atlantic. The British wanted to keep key shipping lanes, like the English

Channel, open to allow its navy complete freedom of movement. The second priority was coastal patrolling to prevent the shelling of ports. And thirdly there was the occasional grand gesture such as the British deployment to the Dardanelles. The war on the Western Front had bogged down into stalemate by spring 1915. The Grand Fleets of both the British and the Germans were predominantly stuck in their ports, because of their shared fear of a catastrophic defeat. Big battleships had become so powerful, and, in the absence of effective bombers, almost invulnerable except to each other and to submarines. So the outcome of a decisive naval engagement would determine the outcome of the war, and this explains the reciprocal timidity of the British and German navies.

The German Kaiserliche Marine made several fruitless sorties into the North Sea in an effort to lure out the British Grand Fleet. The battles of Heligoland Bight, Dogger Bank and Jutland were three direct confrontations: for each of these there were several occasions on which the British and German fleets simply sailed past each other. By the time 1914 turned into 1915, the intelligence analysts in Room 40 had cracked the SKM codes. Initially they found the deciphered messages mainly to be weather reports, or signals announcing the positions of different German ships. Then they discovered that the Germans were sending more precise and operationally important messages – fleet movements, for instance – on short-wave frequencies that British naval intelligence had not been able to intercept. There was no complicated explanation for this. It was a question of allocation of resources. The British began to experiment with direction-finding radio equipment in spring 1915, and intercept stations were built at Lerwick, Aberdeen, York, Flamborough Head and Birchington. The main British listening station that could pick up short-wave radio transmissions from German ships, or military units on the Western Front, was at Hunstanton on the Norfolk coast. Crucial short-wave German naval transmissions were not being picked up simply because there wasn't enough receiving equipment and the aerials weren't big enough. So Room 40 gave the Hunstanton listening station a test for one weekend. They were told to stop listening to routine military messages, like those from German artillery units behind Ypres, or from Zeppelin stations in Belgium, or situation reports from German infantry units estimating which British brigade had moved into the line of trenches opposite them. They were told to focus only on the German High Seas Fleet.

And in forty-eight hours the answer was there. The fleet's movements for two days were being broadcast on short wave using a combination of the SKM code between ships and the HVB code used for messages from the German Admiralty in Berlin to senior officers at sea. It was another breakthrough for the British. As the war progressed, the Germans did this more and more frequently. Their signals key remained unchanged for three months in 1915, but by 1916 it was changed every 24 hours, at midnight. Nevertheless, with huge volumes of intercepted material, several captured codebooks and the knowledge to do it, Room 40 was usually able to break a new key by the next morning, and sometimes as early as 2 or 3am. From October 1914 to February 1919, Room 40 intercepted and solved an estimated 15,000 messages.

•••

Every day the German fleet tended to report the position of each of its ships. Thus, through knowing more or less how many battleships, battlecruisers, cruisers and destroyers the German fleet had, the British could build up a clear operational picture of exactly what the Imperial German Navy was doing: what routes it took, which indicated where minefields might have been lain; what speeds it travelled at; where it re-fuelled. They then discovered yet another flaw in the German coding strategy. Even though intercepted signals showed that the Imperial German Navy knew that the SKM codebooks had potentially been captured from the *Magdeburg*, they were either very slow to change their codes, or simply failed to do it. The VB and HVB codes, whose signal books were captured in the Channel in October 1914, were not to be changed until 1917.[§] The sheer size of each of the books was one reason they could not easily be changed, and the codes continued in use until summer 1916. Even then, ships at first refused to use the new codebook because the replacement was too complicated, so the *Flottenfunkspruchbuch* (FFB) did not fully replace the SKB until May 1917. The Germans were not sure about the security of the SKM codebooks – or, indeed, whether they had been captured from the *Magdeburg* at all. There was an official inquiry into the loss of the codebooks from 1914, after which Prince Heinrich of Prussia, commander-in-chief of Baltic operations, wrote to the commander-in-chief of the German High Seas Fleet, and said he thought it certain that the navy's charts and codebooks had both been captured by the Russians. The Germans were

discovering the flaws of charts and codebooks – once captured, they had to be changed and reissued to every ship and every naval office on land. Secondly, it was sometimes difficult, or just impossible, to discover if the codebooks or charts had actually been captured, leaving the Germans in a dilemma. Assume they had been captured, and change all codebooks regardless? Or take a chance and forego the effort? The fact that the HVB codebook alone was enormous, containing as it did over 300,000 letter groups, was one reason why the Germans simply didn't change it. The logistical complexity of doing so was considered overwhelming. The German reliance on codebooks in World War I, and the subsequent flow of intelligence to the Allies after they were compromised, was going to have a huge impact on Germany's codemakers and codebreakers a decade later, in the lead-up to World War II.

The German Naval Codebreaking Operations

One night in 1914, at the start of the war, a young German naval technician named Wilhelm Tranow was on duty. He was on board in the radio room of the Deutschland-class battleship SMS *Pommern*, one of the five biggest capital ships in the German fleet.[IIII] The radio room received a signal from the cruiser *Breslau.* Tranow forwarded it on to the commanders of the fleet, who replied that they couldn't read it. So Tranow, fiercely interested in cryptanalysis,[¶] codes and codebreaking, decided to try to break the message himself. He succeeded. He forwarded the decrypted message back to his commanders, expecting to be congratulated, or, at the very least, asked how he had succeeded where the radio technicians of the fleet hadn't. Neither happened. He was issued with a stern warning never in future to interest himself in such matters.

The incident was a microcosmic but highly illustrative example of the Imperial Navy's approach. Shortly after this incident, Tranow asked for, and was granted, permission to attend an interview with the Imperial Navy's intelligence service. The *Nachrichtenabteilung,* or 'news' department, was more commonly known by a single-letter abbreviation, 'N'. From 1898 onwards, Admiral Tirpitz had furiously resisted the formation of, and budgeting for, such an intelligence establishment, so that on the outbreak of World War I, it had fewer than ten staff. This number increased enormously from 1914 onwards, but operational efficiency didn't. The most accurate assessment of the department's performance in World War I was that, unlike

its military equivalent, it achieved very little.[**] This was partly because it had no access to any captured Royal Navy codebooks, and partly because the Royal Navy sometimes broadcast its messages in 'clear'. They knew where the German navy was, they had no other maritime enemies in the Channel, North Sea or Atlantic, and Britannia, in 1915, was still very keen to advertise that it ruled the waves. The third reason that the 'N' section achieved little was that it relied on two main sources of intelligence. Listening stations on the Belgian, Dutch and German coasts could pick up Royal Naval signals, but the German naval intelligence network was, at best, too slow to decipher them before the ships had moved. Their second source of intelligence was agents based in foreign ports, such as Piraeus or Istanbul or Shanghai. But as these agents transmitted their own signals in the SKM or VB codes, the British were able to read them.

However, the largest and most damaging fault of the German naval signals intelligence department was its failure to impress upon the High Command of the Imperial Fleet the necessity to change the three main codes they were using, particularly after their radio intercepts increasingly showed that the British had managed to decipher them. Tranow himself, along with some of his colleagues – and of course the entire British staff of Room 40 – could see that Germany's refusal to change its coding system made it effectively obsolete at best, and at worst it helped the enemy.

The Role Played by Signals Intelligence in 1916–17

By sunrise on 31 May 1916, the British Admiralty felt they knew enough about the dispositions and intentions of the German High Seas Fleet to challenge them in open battle. Vice Admiral David Beatty's battlecruisers were steaming towards Jutland. They knew from a combination of signals intercepts when the Imperial German Fleet would leave port, in an attempt to lure Admiral Sir John Jellicoe's Grand Fleet into open battle in the North Sea. But although the codebreakers of Room 40 had proved adept at cracking German codes and reading their signals, the culture of secrecy in the higher ranks of the Royal Navy meant that Room 40's successes did not always have operational impact. This was an example of one of the oldest principles of intelligence: a failure to disseminate its material with operational efficiency meant that the effort made to gather it was wasted, and at Jutland this was felt even at a relatively low level in the British fleet. One British naval

lieutenant who had served on Vice Admiral Beatty's flag-ship, HMS *Lion*, between 1914 and 1915 said that only a small number of decoded intelligence reports actually reached the Grand Fleet in time to have any effect.

The Battle of Jutland was an enormous confrontation in terms of numbers: 151 British vessels, including twenty-eight battleships and seventeen heavy cruisers, were involved. The Germans fielded ninety-nine ships, including sixteen battleships and eleven heavy cruisers. Signals intelligence meant that the British arrived off Jutland before the German submarine picket had time to get into place. The battle could have been the decisive naval engagement that affected the outcome of the war, but it ultimately lacked a decisive conclusion: both sides claimed they had won, although the British lost twice as many ships and twice as many sailors. However, the Germans didn't manage to destroy a significant part of the British fleet, and the British managed to contain the German navy. Thereafter, the latter could not gain access to the Atlantic, and so had to rely on submarine warfare and attacks on Allied and neutral shipping. And in this, the Germans were to have the upper hand. The reversion to a reliance on submarine warfare was in turn to lead to the British development of the convoy system, and this itself would become inextricably linked with codebreaking in the Second World War. Jutland would, in effect, cast a long shadow.

Despite their capture by the British, the VB and HVB codebooks continued to be used until after the Battle of Jutland, which turned out to be the only naval confrontation of any size involving battleships during World War I. The Germans then also compounded their errors. They made the mistake of transmitting information about codes and codebooks in wireless messages whose codes had been broken by the British. Orders to change the crucial monthly 'key' on a substitution table were sent out by wireless in the 'old' cipher, which the British had broken. The instruction was then repeated in the 'new' cipher. So if the message written in the old cipher said, '*Alphabetic Substitution for February 1915 will commence as A on G through encipherment T repeating on J …*' British codebreakers thus had a very substantial seventeen-word and letter 'crib' into the new cipher. And in ten months in 1915, for instance, the Germans only changed their key codes six times.

Submarine Warfare and the Convoy System

By the middle of the war, the British had a very clear upper hand over the Germans when it came to naval codebreaking. With the armies of both sides bogged down in a stalled war of attrition on the Western Front, maritime operations were one area where flexibility of movement and action was still possible. When it came to submarine warfare and the struggle against domestic supply convoys, however, it was the Germans who were in a dominant position. This was a situation that was almost to cost the British the war. Although naval vessels like battleships never left harbour without destroyer escorts, the crucial merchant ships that kept Great Britain supplied with over 60 per cent of its food supplies went unescorted. The country imported meat, wheat, butter and fruit, all its oil came from the Persian Gulf and Libya, most of its iron ore from Norway, while its other minerals such as bauxite and phosphates, and metals such as magnesium, zinc and copper, were imported too. The vessels that carried all these foodstuffs and raw materials were left to steam across the Atlantic and the North Sea by themselves, and by the middle of the war German submarines were sinking them almost faster than they could leave harbour. The lack of convoy escorts stemmed from an outdated single-issue focus on the part of the heads of the British Admiralty. They were obsessed with the idea of offensive battle: of finding and destroying the enemy's fleet. They considered the protection of convoys and the British coastline to be defensive, a very secondary consideration. The most important factor was the Royal Navy's refusal to consider the submarine as a weapon that could cause massive economic damage, rather than just defend harbours and warships. Apart from Admiral Fisher, the British closed their eyes to this. On New Year's Day 1914, Winston Churchill for instance said that he could not think that sinking merchant ships would ever be done by a 'civilized power'. Along with Germany's dogged determination to continue using codebooks that could prove to be compromised, the Allies' lack of understanding in World War I of the efficacy of submarine warfare and their resistance to adopting the convoy system were two factors which were going to have an enormous impact on the Battle of the Atlantic more than twenty years later.

In 1915, the British and Allied merchant navies lost over 400 ships – amounting to more than a million tons – to German submarines. By 1916 this figure had nearly doubled, to 964 ships, and nearly two million tons. It was only by the end of October 1916 that the commander of Britain's Grand Fleet, Admiral Jellicoe, saw the truth. It wasn't a question of defeating the

German fleet in open battle, but of destroying the unseen submarines. Otherwise, regardless of the progress of the land war on the Western Front, Britain faced defeat and semi-starvation: this was to prove as important in the next war to come twenty years later. On 29 October 1916 Jellicoe wrote to the First Lord of the Admiralty:

> There appears to be a serious danger that our losses in merchant ships, combined with the losses in neutral merchant ships, may by the early summer of 1917 have such a serious effect upon the import of food and other necessaries into allied countries as to force us into accepting peace terms, which the military position on the Continent would not justify and which would fall far short of our desires.[4]

But the admirals commanding the Royal Navy still considered the convoy system impractical. They didn't understand it, and they didn't understand submarines. And so, when the Germans resumed unrestricted U-boat warfare on 1 February 1917, they estimated that such was Britain's reliance on imported food and goods, and such was the capacity of submarines to sink merchantmen, that within five months they could destroy more than 40 per cent of the country's imports. The rate at which Allied merchant ships were sunk in the following three months backed up this assertion: German U-boats proceeded to sink around 600,000 tons of shipping per month from February to April. One of the submarine commanders in the Imperial Navy at this time was a Captain Karl Dönitz, who noted quite how fast and how effective U-boats were against unprotected merchantmen. And the cost to the Germans of this operation? Eight U-boats. By the end of February over 600 ships in various Allied ports were refusing to put to sea.

When the United States came into the war in April, the situation had become desperate. Not only was Britain incapable of protecting its commercial maritime supply lines – and thus facing starvation or surrender – it also couldn't guarantee to be able to supply its armies thirty miles away across the Channel. But with America coming into the war, there was a faint chance the geo-strategic situation could improve, as the United States could provide escort ships and convoys could form up in harbours on its eastern seaboard. If the convoy system was adopted, Britain's key ally in the war – France – could also continue to be supplied with coal from England, but if not, the the French armaments industry would simply collapse. The stubborn

naval old guard in the British Admiralty had no choice. Defeat, brought about not in the heat and bravery and derring-do of battle, but on the front lines of gritty economic reality, was staring them in their faces. In May and June 1917, five convoys left the United States with escorts. There were seventy-three ships in them. Only one was torpedoed. Seventy-two reached the British Isles safely. The convoy system was officially adopted.

The Zimmermann Telegram, 1917

In no single incident in World War I did the British signals intelligence operation achieve so much, nor have its entire strategy so comprehensively vindicated, as in the Zimmermann telegram affair of early 1917. And in no single incident did every German failing in coding strategy since 1914 do them so much damage. On 11 January 1917, the German foreign secretary composed a telegram. It was enciphered in the diplomatic code the Germans used. Arthur Zimmermann, their foreign minister, wanted to send it to the German ambassador in Mexico City. The Battle of Jutland had seen the British navies effectively deny the Germans definitive strategic control of the North Sea and the Atlantic. The Imperial German Navy had decided that submarine warfare against Britain and, in particular, the United States was their next strategic step. They imagined correctly that this would lead to war with America. Zimmermann told the ambassador in Mexico that if and when the United States entered the war on the British, French and Russian side, he, the ambassador, was authorized to make a proposition to the Mexican government. The famed 'Zimmermann telegram' laid out an extraordinary plan. The Germans would give the Mexicans funding and a military alliance designed to destabilize America's military capacity and its desire to fight a war across the Atlantic. A successful outcome would see the Mexicans rewarded with parts of American territory.

'We intend to begin on the first of February unrestricted submarine warfare,' wrote the German foreign minister:

> We shall endeavour in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and

Arizona. The settlement in detail is left to you …[5]

Irony then played a huge hand. Because in 1911 the British had pre-emptively cut the five principal trans-Atlantic wireless cables, the message had to be delivered to the United States Embassy in Berlin. The Germans could not send it directly. But they had diplomatic permission to 'piggy-back' on the Americans' diplomatic wireless cable service. Normally the Germans simply handed in messages in clear text to the Americans, who relayed them to the US embassy in Copenhagen, and thence across the Atlantic. The American government had only allowed the Germans to communicate in this unique way because they thought it might make forthcoming peace negotiations logistically easier. For their part, astoundingly, the Germans assumed the American cable service was secure. But on this particular occasion with the Mexican telegram, the Germans understandably insisted that their message be coded. So a telegram from one wartime party discussing with a third party – Mexico – about the territorial division of another country was sent on that same country's communication system. It left Berlin on 16 January 1917.

What neither the Germans nor the Americans knew was that Nigel de Grey and Room 40 were listening. Before being transmitted across the Atlantic, the cable from the US embassy in Copenhagen had to pass through a relay station at Porthcurno near Land's End. And everything that went through this relay station on the westernmost tip of England was copied to Room 40. De Grey and his colleagues had deciphered much of the 'Zimmermann telegram' by the following day. He used the German diplomatic codebook, code-numbered 13040, that had been captured in Mesopotamia in 1915, as well as the original SKM codebook from the *Magdeburg*. Two days later Admiral Hall had, through three different and circuitous routes, made the contents of the telegram public. It coincided with the start of German submarine attacks on American merchant shipping, and saw America unsurprisingly join World War I on the side of the Allies.

•••

Signals intelligence from 1914 onwards had thus altered the course of World War I; it had also altered the operational fate of the German Imperial Navy, and was to affect its World War II successor, the Kriegsmarine, in a huge and

completely unexpected way. The shots fired by the *Magdeburg* were the first not only of the war, but of a different, more modern and complex conflict for the Germans that was to grow and develop exponentially over the next thirty-five years. It was the huge rivalry centred on signals intelligence, and the making and breaking of codes. As World War I progressed, so all sides were fast becoming aware of the five cardinal imperatives of cryptanalysis and signals intelligence. Break the enemy's codes fast and often, don't let him know they are being read, if your own codes risk being broken change them again and again, disseminate any gathered intelligence to the correct recipients as fast as possible, and make sure they can and do act on it. But neither the Germans nor the British always obeyed these rules, and so their actions were to have long-lasting effects that would go a long way to dictate how the huge and vital signals intelligence war was fought in World War II. Germany, in particular, was to make enormous efforts to ensure that the catastrophic errors it had made in signals intelligence in World War I were never repeated, and one of the most crucial decisions was to replace codebooks with encrypting machines, like the Enigma system. In 1919, the German codebreaking apparatus started to rebuild itself in the aftermath of the Treaty of Versailles. And one man in particular kept the failure and humiliation of the Zimmermann telegram in mind. Somebody who that year was looking to the future, a technician already at work trying to break some of Royal Navy's codes: Wilhelm Tranow.

---

* The copy of the SKM codebook held in the National Archives (no. 151) is not sea-stained – Christopher Andrew in his book *Secret Service: The Making of the British Intelligence Community* (Heinemann, London, 1985) says the Russians simply gave the British the dry codebook from the captain's safe. In photographs the SKM codebook does not appear to have suffered salt-water damage.

† The American mathematician Claude Shannon summarized it in 'Shannon's Maxim' when he said 'assume the enemy knows the system'.

‡ Denniston went on to become the first head of Britain's Government Code and Cypher School.

§ The post-World War I German naval surveillance service, the B-Dienst, produced a report into the loss of the *Magdeburg*'s codebook twenty years later. The German report, produced in 1934 by one Corvette Captain Kleinkamp, found that the

capture of *Magdeburg*'s SVB codebook had been 'disastrous', mostly because the German navy took no steps to replace the codes with new secure ones.

‖‖ All ships in the Imperial German Navy were designated SMS, for *Seiner Majestät Schiff*, His Majesty's Ship.

¶ *Cryptanalysis* comes from the Greek words *kryptós*, 'hidden', and *analýein*, 'to loosen' or 'to untie'. It is the study of analysing information systems in order to study the hidden aspects of the systems. Cryptanalysis is therefore to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

** This was an assessment that the section in fact awarded itself in 1916, after the German failure to intercept and decipher any British signals concerning the movement of the British Grand Fleet before the Battle of Jutland.

Chapter Two

THE ENIGMA SALESMAN

Arthur Scherbius was an electrical designer from Frankfurt, and an early twentieth-century German engineer whose inventions included the electrically heated pillow. He made parts for turbines as well, and thought of new methods of manufacturing heating elements that passed through ceramic fittings. His company enjoyed some small and limited successes, although the heated pillow never quite broke into the market for bedding materials in Germany and Switzerland. He then turned his mind to inventing things that could potentially have a commercial application in the military world. It was 1918, and Germany was nine months short of losing World War I. In February of that year, the forty-year-old Scherbius filed a patent for a cipher machine. He called his latest invention 'Enigma', after the Latin word for 'riddle', or 'something mysterious'.

It worked by taking an electrical current and passing it through a series of plugs and an alphabetic keyboard connected to a number of different rotors. The operator would type in the message to be encoded, the rotors would spin it through a constantly changing combination of alphabetic possibilities, and out would come the enciphered text, letter by letter. The text could then be deciphered by doing the same thing backwards. Such was Scherbius' basic idea.

Shortly after he filed his application for a patent, the German naval intelligence service – 'N' – wrote to him. Could he, they asked, come to their

headquarters and give a select group of officers a demonstration of his new machine? It was the moment he had been waiting for. Naval intelligence were desperate to find a way out of their dependency on the old, flawed system of codebooks which had created a cryptanalytical and cryptological gridlock where the British had a strong upper hand. The German naval intelligence service were looking for any new mechanical system they could find that could replace it. So Scherbius travelled to the headquarters of 'N' in Berlin, where a group of officers and civilians were waiting for him. Among them was Wilhelm Tranow.

Scherbius had brought one of his prototype machines with him. It was what he called the Model C. His first version had been the size of a cash register, and weighed nearly forty pounds. But the model he brought to the meeting was smaller, measuring a foot by six inches by four-and-three-quarters, and it looked like nothing more than a lumpen typewriter with two keyboards in a wooden box. Scherbius demonstrated it, explaining as he went along how it worked. The principal component, he said, was a rubber and metal disc with two flat sides. On one side were twenty-six electrical contacts, and on the other twenty-six more. As many as eight discs could be used in later Enigma machines, but in Scherbius' prototype three or four could be inserted. A series of wire links led through the discs, connecting them in pairs at random. Two metal plates held the discs between them, one of them receiving electrical current from a typewriter keyboard, the other sending the current onwards to a panel which had twenty-six small glass-covered apertures on it, each bearing a different letter of the alphabet. This disc was the 'rotor', the operational basis of the machine. It was threaded onto a spindle, so that the electrical contacts on both sides of the rotor connected the keyboard to the panel. When a key was pressed on the keyboard, a different letter would light up on the panel. Which letter this was would depend on the wiring within the rotor, and the position in which the rotor was placed on the spindle. In its initial position, therefore, the rotor effected a simple monoalphabetic substitution. If the letter B was pressed on the keyboard, the wiring on the rotor would connect it to whichever other letter of the alphabet had been decided by the person wiring the rotor.

Say B was connected to Y: if so, then when B was the first letter pressed on the keyboard, the second letter Y would light up on the panel. However, after each letter key was pressed and illuminated, the rotor would advance on the spindle by one twenty-sixth of a turn, providing an entirely different set of

permutations. If the letter B was now pressed again, not Y but another letter would be connected to it, and that letter would be illuminated on the panel. Then, the rotor would advance again, changing the permutations once more. With one rotor, the machine would be able to arrange the permutation of letters available, which was obviously twenty-six. It could encode the alphabet in twenty-six different ways before returning to its initial position. But if a second rotor was added, this increased to 26 x 26, or 676 possible combinations, for the first letter pressed on the keyboard was directed through the first rotor, the second through the second, the third through the first, with each rotor turning once after each letter selection. With a third and fourth rotor added, the number of combinations of letter that could come from one press on the letter K, say, on the keyboard, was always twenty-six to the power of the number of rotors placed on the machine. With three rotors, this was 17,576, with four, 456,976. And each time the operator set up the machine at the beginning of each day or coding session, he could choose the setting of each rotor, thus deciding the starting position of each letter on it.

The Enigma machine had a patented feature making it different from other rotor devices, which made messages attractively easy to read for the receivers, as long as they knew the settings in use. This was an additional disc called a reflector, which returned the current back through the same set of rotors, matching the letters of the alphabet in reciprocal pairs. If A, for example, was enciphered as K in a given setting of the machine, then K would be enciphered as A. This meant that the operator receiving a message needed only to key in the cipher text to be able to read off the plain text on the illuminated panel. One consequence was that no letter could be enciphered as itself in plain text: A could never be cipher text A, and so on. This would later prove to be a decisive weakness.

'The key variation is so great,' Scherbius wrote, 'that, without knowledge of the key, even with the available plaintext and ciphertext, and with the possession of the machine, the key cannot be found, since it is impossible to run through 6 billion or 100 trillion rotor starting positions.'[1]

The naval intelligence officers announced that they thought it afforded good security, even if compromised. But it was too complex, too cumbersome, they said. And too costly. Scherbius was asking for between 4,000 and 5,000 Reichsmarks per machine.[*] This was hugely in excess of 'N's rather modest budget. They knew that if they bought Enigma machines to equip their department, then the entire German navy would have to follow

suit. It was too late in the war to equip a whole fleet with a complicated new means of covert communication. Why not, said one of the officers, try the Foreign Office? They may be interested in it for the encryption of diplomatic traffic. So Scherbius tried to arrange a meeting with the government ministry. They declined. The war was as good as lost and they had neither time nor budget. They were content to rely on their codebooks and telegrams, even after the decryption of the Zimmermann telegram had helped to bring the United States into the war the previous year. This had demonstrated very clearly the reliance of Germany's government ministries on insecure methods of communication.

Arthur Scherbius had therefore set up his own company called Chiffriermaschinen Aktiengesellschaft to manufacture the Enigma machine. The title translated as Cipher Machine Joint Stock Company. He decided to try to sell his invention to two of Germany's neighbours: Switzerland and Poland.

The Treaty of Versailles and Germany's Economic Collapse

By summer 1918 American troops were arriving in France at the rate of a division a week. In the face of these vast resources, the German army's reserves were non-existent. The country was broke and the population on the breadline; the Allied maritime and land blockade meant Germany could not import food to eat or raw materials to produce any goods for export. Whereas U-boats had nearly brought Britain to its knees, British destroyers and frigates enforcing an economic blockade had almost suffocated Germany. In late October 1918 sailors in the Imperial Navy in Kiel mutinied, and along with soldiers and factory workers they began organizing themselves into socialist groups modelled after those formed in Russia just after the revolution in 1917. The rebellion in Germany spread, and by November riots and street fighting had reached Munich. The workers demanded that Kaiser Wilhelm II abdicate, and the German armed forces supported them, declaring that they were no longer strong enough to back him in power. On 9 November a German Republic was installed and the Kaiser duly abdicated. The armed forces surrendered and on 11 November 1918 at 11am the Armistice came into effect. One British corporal on the Western Front later remembered that the Germans in the trenches opposite his unit simply walked across No-Man's-Land, stood in a line, and bowed to the British soldiers. And then

simply walked back to their positions and prepared to return to a defeated Germany.

Inside the country, street fights and riots between left-wing parties and the army continued until 19 January 1919, when National Assembly elections took place. To avoid the continuing disorder in Berlin, the assembly convened in Weimar, a coalition government led by moderate democrats was installed, and the new republic had its name. However, everybody simply continued to call their country the German Republic. The first president, the Social Democrat Friedrich Ebert, signed the new constitution on 11 August 1919. One world war was over, and very shortly the Treaty of Versailles was going to begin to push Germany towards the next one. The implications of the treaty for the future of Germany's signals intelligence service were enormous, and the manner in which the army, navy, air force and Foreign Office's cryptanalytical departments were going to develop in the run-up to World War II was profoundly influenced by the ramifications of the treaty's clauses.

The Armistice that came into force on 11 November 1918 might have ended the fighting between Germany and the Entente Powers, but it would take six months of negotiations by the victors at the Paris Peace Conference to finalize it. The eventual signing of the Treaty of Versailles in June 1919 put a formal end to the war. The Imperial Army was dissolved. Various right-wing paramilitary groups made up of war veterans, called the Freikorps, continued to exist while a new army, called the Reichswehr, or 'defence of the realm', was instituted on New Year's Day 1921. The Versailles Treaty stipulated that Germany could have no more than 100,000 soldiers in seven infantry and three cavalry divisions, along with ten light armoured vehicles and thirty-six ships of all sizes. General Hans von Seeckt, the new head of the army, stated immediately that his men were not loyal to the new Weimar Republic, which he blamed for betraying Germany, humiliating its people and allowing the British, Americans and French to punish the country for starting the war. The German people, he said bluntly, had been stabbed in the back.

One of the most important clauses of the treaty was Article 231, which would have a significant effect on the future of Germany's signals intelligence and cryptanalytical capability over the next twenty-five years. This article of the treaty became known as the 'War Guilt' clause. It obliged Germany to assume financial responsibility for all the damage caused during the war, and

to pay 132 billion German marks in reparations. This was equivalent to £6.6 billion in 1919. (Nearly 100 years later in 2017 it was worth some £280 billion.) Germany had to disarm, make territorial concessions on both eastern and western borders, limit the size of its armed forces, and pay huge reparations. By March 1920 the force of 100,000 men Germany had under arms was supposed to make it incapable of offensive military action. The Rhineland was demilitarized, and military structures on the islands of Heligoland and Dune, where the German army had two of its signals listening stations, were ordered to be demolished. The number of men allowed in such units as signals intelligence was slashed. The navy was only allowed to have a total of twenty-four battleships, cruisers and destroyers, and twelve torpedo boats. The number of sailors was reduced to 15,000. The subsequent impact on the wartime German signals intelligence establishment was drastic and immediate. Essentially it ceased to exist. 'N', the naval intelligence division, was disbanded. The 1,200 men serving in the army's cipher unit were demobilized, and as the army had handled much of Germany's diplomatic signals traffic during the war, this capability disappeared as well. But for Arthur Scherbius, travelling between Switzerland and Germany and Poland trying to sell his Enigma machine, this demilitarization, paradoxically, made his job significantly easier. The fewer personnel there were in the German armed forces, the fewer Enigma machines they would have to buy to equip them. If there were only twenty-four main ships in the navy, that meant only twenty-four Enigma machines for them. However, Germany's subsequent economic collapse was going to make it much harder for the country's new armed forces to pay for them.

Faced with the payment of huge war reparations, the German economy nosedived. In 1914, when World War I broke out, Germany made the enormous political-economic error of suspending its Gold Standard. This was the convertibility of a single unit of its currency – the mark – into gold. The German emperor and parliament decided to fund the whole war by borrowing, predominantly from the Americans. They thought they would be able to repay the loans by winning the war, taking over new industrial territory on their eastern and western borders, and imposing war reparations on the Allies. This reckless strategy backfired when they lost. They couldn't export goods because they didn't have the money to produce them, partly because they couldn't afford to pay the labour force. And the Allied economic blockade of Germany meant that the Germans could not import food,

manufactured goods and raw materials. Quite simply, the country had borrowed exorbitant sums to pay for the war that it now could not pay back. The mark devalued against the dollar from forty-eight paper marks in 1919 to ninety in 1921. In May of that year, the London Ultimatum decreed that Germany had to pay its reparations in gold or foreign currency, neither of which it had. So Germany started printing more paper money to buy hard foreign currency; inflation led to hyperinflation; and by Christmas 1922 it took 7,400 marks to buy just one dollar.

Germany then tried to pay its reparations in hard commodities such as coal, but when workers in the Ruhr valley went on strike after French and Belgian troops occupied the area in January 1923 to enforce reparation payments, hyperinflation got even worse. The government printed more money to try to pay these workers. By November of 1923, the American dollar was worth 4,210,500,000,000 marks. Photographs appeared from Germany of men pushing wheelbarrows full of money to buy a loaf of bread, or using the effectively worthless money as wallpaper.

Helmut Ruge[†] was born in 1917, the eldest child of parents in the northern town of Cuxhaven, where his father worked in the Port Authority:

> I can remember very well going each week with my mother and my sister to the offices of the Port Authority where my father worked as a ship's carpenter, carrying baskets in which to put the 'mountain' of paper money he had earned that week. After receiving the money we would run to the shops to buy food and whatever else we needed as quickly as possible, because the next day the money had devalued further and the food we could afford to buy was less.[2]

Yet even in this extraordinary economic environment some businessmen continued to make money. One industrialist, who insisted he be paid in dollars, built up an empire of more than 200 factories which produced the huge amounts of paper needed to make the bank notes that were being printed in their millions to fund this inflation.

In this harsh and unforgiving economic environment, Arthur Scherbius was trying to sell a complex, expensive and revolutionary piece of communications equipment. Not to be discouraged, he saw a gap in the market: he realized that German companies would need to communicate secretly with foreign business partners and banks about new inventions,

contracts and deals. Banks, particularly, needed a confidential form of communication for currency deals and money transfers. Why not try to interest them in the Enigma machine? Excited by this thought, he bought another patent, for a cipher machine similar to his own that had been designed by a fellow German. Now, he decided, it was time to start selling it effectively. But Germany's business leaders were concentrating on more basic fundamentals: having enough copper and aluminium from which to make telephone wires, for instance, so that they could even continue communicating by telephone and telegram. It was too early for Enigma.

Still, the engineer from Frankfurt who had invented the electric pillow was not to be deterred. He saw that although the Treaty of Versailles had effectively barred Germany from running intelligence agencies for its armed forces, his former potential clients at the naval intelligence division had proceeded to create a brand-new unit. Clearly some funding, from somewhere, was available. Gone was 'N', the old news department. Now there was a small group of eight officers and civilians, led by Wilhelm Tranow. Scherbius decided to have another attempt at interesting them in his machine. Other inventors in America, Holland and Sweden were working on a rotor-based device similar to his. He didn't want to miss out on potentially lucrative contracts supplying Germany's new armed forces, and, he realized, if the navy began buying then so would the army and, he hoped, the Foreign Office. It was premature to think of selling his invention to the German air force, as the Versailles Treaty had stipulated that Germany couldn't have one.

Wilhelm Tranow and the Rise of the B-Dienst

The German naval intelligence division – 'N' – was now disbanded. Its former head of foreign intelligence gathering had closed its headquarters at Neumünster on the northern Baltic peninsula. However, the staff returned to Berlin to discover, to their surprise, that the navy had decided to form a new signals intelligence bureau as part of its new and secret naval intelligence agency. They called the new unit the Beobachtungsdienst, or observation service, shortened by everybody to B-Dienst. On paper, the new office was created in April 1919 at exactly the same time as the Reichsmarine, the new German navy, was born, but in reality it was to take until 1923 before it started to become operational. Rear Admiral Adolf von Trotha, who commanded its new intelligence service, saw that the new unit needed only a

very small budget to run a few intercept stations on the North Sea and Baltic coasts, and a central deciphering unit. On the navy's twelve battleships and cruisers, radio monitoring and interception would be carried out by the ships' signals personnel using a radio direction finder to track the outgoing messages of vessels from other navies. Von Trotha set up the B-Dienst in a small headquarters near the German naval academy at Flensburg-Mürwik, which lies on the Baltic Sea exactly where the borders of Germany and Denmark meet. The agency then got to work gathering its information. It did this in four main ways.

The first thing the new German unit did was to try to find out how successful the British had been in intercepting and decrypting their coded signals in World War I. Tranow and the other seven cryptographers from the B-Dienst read as many British publications as they could which dealt with signals intelligence. Amongst these were the memoirs of the British admirals who had commanded battle fleets in the war, publications such as *Naval Operations* and the autobiography of Admiral Sir John Fisher. There was also Winston Churchill's series *The World Crisis*, the first two volumes of which were published in 1923. In this Churchill had recounted a slightly over-dramatized version of the capture of the German naval codebooks from the SMS *Magdeburg*. Exaggeration apart, the Germans started to realize exactly how thorough had been the British decryption of their naval signals. Admiral Fisher alluded in a very general way to signals decryption in his autobiography *Memories*, published in 1919:

> The development of the wireless has been such that you can get the direction of one who speaks and go for him, so that the German daren't open his mouth. But if he does, the message is in cypher, and it is the elucidation of the cypher which is one of the crowning glories of the Admiralty work in the late war. In my time they have never failed once in that elucidation.[3]

The second thing the B-Dienst did was to try to pick up as much new naval radio traffic as it could. The Admiralty set up ten intercept stations on the North Sea and Baltic coasts, ranging from large ports such as Kiel and Wilhelmshaven, to small harbour towns like Borkum and Swinemünde, rain-swept in winter, wind-blown in summer. The B-Dienst's main targets were the British, French and Russian navies, with the Royal Navy and the British

Merchant Navy its priorities. Every time a ship from one of these fleets appeared in the North Sea or the Baltic, the listening stations would lock onto its radio traffic. Intercept stations were also established as far south as possible to monitor ships sailing in the Mediterranean. This was the early 1920s: the terms of the Treaty of Versailles specified that Germany was forbidden any form of armed forces intelligence agencies. As such, the southern monitoring stations could not be in the demilitarized area of the Rhineland, unless the German naval operators were prepared to physically camouflage their aerials and wireless antennas. Instead they chose a small village in the Black Forest.

The third action taken was to improve methods of gathering information about the movements and signals of foreign navies outside of the Baltic, the North Sea and the English Channel. This came from German agents based in ports around the world. Since before World War I, the German navy had relied on a network of diplomats, naval reserve officers, businessmen and employees of shipping lines to pass on information to them about the movement of other countries' vessels, particularly ships from the British Royal and Merchant Navies. These part-time agents worked either for the national interest, in the case of naval reservists and diplomats, or for money, in the case of shipping line employees, maritime clerks and other port officials. Before the war they had been happy to do this work as it often led to preferential treatment in the awarding of lucrative naval cargo contracts. These agents were based in every port in the world from Shanghai to Trondheim, Montevideo to Basra, and Piraeus to Cape Town. With their ledgers and their lists, in tropical autumn, Mediterranean spring, Arctic winter, and the baking heat of a Red Sea summer they watched every vessel arrive in harbour, drop anchor, dock, tie up, load cargo, and unload cargo. Whether it was the leopard-like lines of a grey destroyer, the trudging slump of a tramp steamer hauling coal or cement, or a huge and magisterial cargo ship moving grain or oil by loads counted in thousands of tons, these people knew ships, they knew the sea and they knew the shipping world. They saw everything and they kept watch, and kept notes. So German naval intelligence went back to this agent network that had existed before and during World War I, and they passed word about what they wanted. The names of British merchant ships passing through port each day, and if possible any sightings of British naval vessels, where they were headed, and whence they came. Tranow and his men were about to start trying to break the codes of the Royal Navy,

and this information would be their way in.

The fourth way the B-Dienst saw they that could gather information about the movements of British, French and Russian ships was to monitor the signals they sent when they were on manoeuvres and active service. The wheel had come full circle: the German navy had lost the cryptological advantage in World War I because of its dogged reliance on codebooks, and its refusal to change them frequently enough. Tranow saw that the British Royal Navy seemed determined to go down the same path, and he was keen to exploit this failure. But the B-Dienst themselves, and the new German navy, needed secure communications too. What system were they to use? And how were they to pay for it?

The Lohmann Plan

From 1923 onwards, the German Reichswehr secretly approved millions of 'gold marks' worth of funding for a wide variety of naval, military and air force projects which explicitly broke the terms of the Treaty of Versailles.[4] The German defence minister, Otto Gessler, and Admiral Paul Behncke, Chief of the Admiralty, were in charge. The German economy was still moribund, the scheme contravened the Versailles Treaty and so the plan was hidden from parliament. One part of it, for instance, involved the creation and maintenance of a parallel German naval intelligence service. Another oversaw submarine and ship design. A third aircraft building. The total 'black' funding for these rearmament projects amounted to some thirty million dollars-worth of marks. The navy financed twenty-five million marks from its own reserves of foreign currency and gold marks – i.e. German marks backed up by existing bullion deposits, sometimes in foreign banks that were untraceable by other parts of the German government. In turn, much of this money came from selling submarines and warships, and parts thereof, to third parties in Italy, Scandinavia or South America. Given that many of the German navy's vessels had to be physically scrapped in keeping with the Versailles diktats, it made it easier to pretend they had been reduced to scrap metal when in fact they had been sold to other countries' navies. When the French army occupied industrialized parts of the Rhineland, the German parliament, the Reichstag, voted another two-and-a-half million for the navy. These so-called 'Ruhr Funds' were designed to strengthen the armed forces as they expanded beyond the restrictions of Versailles. Private businessmen and

right-wing political parties gave another two-and-a-half million.

The money for the covert rearmament was held in a German bank, Berliner Bankverein, which acted as a middleman between the navy and the army, and the companies and agencies that actually received money and implemented projects. The German navy put Captain Walter Lohmann in charge. He was the son of a former director of the North German Lloyd shipping line, and in World War I he had served with distinction as a logistics specialist, undertaking risky and high-profile diplomatic missions. In 1920 he went to St Petersburg by ship and negotiated with the Russians to release impounded German merchant ships which he then used to run sanctions-busting food supplies to Germany. He also went to meet officers from the Red Army who were running ad hoc prisoner-of-war camps outside the city, where German POWs – military, naval and civilian – were still being held.

In October 1920 Lohmann took command of the Naval Transport Division at navy headquarters in Berlin: the commander-in-chief of the new Reichsmarine, Admiral Paul Behncke, trusted him. He considered him an honourable German patriot and naval officer whose duty it was to assist with the rebuilding and rearming of the country's armed forces in the wake of the crushing national humiliation imposed by the Versailles Treaty. Behncke put Lohmann in charge of the 'black' funds in early 1923. Under his supervision, naval, military and new air force projects that broke the terms of the Versailles Treaty were planned, financed and set up. Lohmann proved to be a good planner and a canny logistician who, at the outset, chose projects wisely, funded them adequately and discreetly, and pushed forward Germany's rearmament in imaginative and far-thinking ways. One of the sub-projects, for instance, was a fake company called Mentor Bilanz. This was a front for three German shipyards which, with funding from Lohmann, operated a highly successful submarine design office in the Netherlands. Both Lohmann and a naval officer called Captain Wilhelm Canaris then arranged for one of the submarines designed by Mentor Bilanz to be built at Cadiz in Spain. Captain Karl Dönitz was one of Germany's naval officers who had first-hand knowledge of how successful submarine warfare had been in the last war, and he was now determined to repeat it in the event of another conflict. Under the guidance of himself and other submarine officers, Germany was specifically trying to design a medium-size submarine that could fire a torpedo without the gas from the torpedo tube leaving a huge air bubble on the surface that betrayed the submarine's position.

The funding from Berliner Bankverein also went into trying to set up a network of intelligence agents in former enemy countries – Russia and France specifically – where Germany was not allowed to have a naval attaché, and to funding the already existing German naval intelligence network in ports across the world. For if the naval intelligence agents were looking for British ships' movements to pass on to the B-Dienst, it was because Wilhelm Tranow was looking for more than just the ships' dates of sailing or latest ports of call. He was looking for ships' precise positions. From 1919 onwards he was trying to reconstruct not just Great Britain's Merchant Ships Code‡, but its enormous Government Telegraph Code, which Royal Navy warships used to send their daily position reports. If he could decrypt these, he could begin to work out the exact position, each day, anywhere in the world, of every ship in the Royal Navy.

The encryption and decryption techniques that Tranow and others used were varied but the fundamental principles were the same. Although the language in question obviously varied depending on the cryptanalytical unit in question, be it German, French, Turkish or English, cryptanalysts themselves used the same coding techniques, whose basic principles and techniques were as follows:

Ciphertext-only is a text where the cryptanalyst only has access to a series of already-encoded ciphertexts or codetexts.

Known-plaintext is a text where the cryptanalyst has a set of coded ciphertexts to which he knows the corresponding plain text.

Cryptanalytical attacks can be classified based on what type of information the attacker has available. As a basic starting point it is normally assumed that, for the purposes of analysis, the general algorithm is known: this was equivalent to Kerckhoffs' principle.

Frequency analysis is the basic tool for breaking most classical ciphers. In natural languages, certain letters of the alphabet appear more often than others; in English, E is likely to be the most common letter in any sample of plain text. Similarly, the digraph TH is the most likely pair of letters in English, and so on. Frequency analysis relies on a cipher failing to hide these statistics. For example, in a simple substitution cipher (where each letter is simply replaced with another), the most frequent letter in the ciphertext would be a likely candidate for E. Frequency analysis of such a cipher is

therefore relatively easy, provided that the ciphertext is long enough to give a reasonably representative count of the letters of the alphabet that it contains.

Polyalphabetic substitution is a technique whereby one set of letters is substituted for another. A plain text set of letters is substituted for another, as previously explained, in a *monoalphabetic* substitution. In a polyalphabetic one, this first enciphered alphabet is again substituted for another, so it is effectively encoded twice.

Indicators. Reciprocal machine ciphers such as the Enigma machine meant that each message had its own key. Usually, the transmitting operator informed the receiving operator of this message key by transmitting some plain text and/or ciphertext before the enciphered message. This is termed the indicator, as it indicates to the receiving operator how to set his machine to decipher the message.

Depth. For an operator to send two or more messages with the same key is an insecure process. To a cryptanalyst the messages are then said to be *in depth.* This may be detected by the messages having the same *indicator* by which the sending operator informs the receiving operator about the key generator initial settings for the message.

Subtractor tables are used to encipher a message. The person sending the message can use groups of two, three, four or five numbers to represent a word. In a codebook, as in a dictionary, words would be listed against the numbers used to encrypt them. If the code in question was a four-figure one, for instance, the number 6328 could represent the word 'cruiser'. To encipher this, the number above is subtracted from the daily 'key' number to which it corresponds – say 9883 – producing the number 3555, which the radio operator sends to represent the word 'cruiser'. A fuller description of the encoding or deciphering process using subtractor tables is included in Chapter 5.

•••

As explained previously, Tranow had spent some time as a battleship radio operator during the war monitoring and trying to decipher British codes. Eight years later, in the newly established B-Dienst, he had three very clear ideas of how British codes functioned and were used. Every day each ship in the British merchant fleet and the Royal Navy sent a radio message to London with its position wherever it was in the world. The merchant ships

sent theirs to their respective companies and to Lloyds of London, the warships to the Royal Navy's headquarters at the Admiralty in Whitehall, and in Portsmouth. Tranow knew that almost all British merchantmen sent the same message every day with the ship's name, the words 'position report', the date and the coordinates in longitude and latitude. So a freighter called MV *Sirius* would radio in a dispatch that said '*MV Sirius position report midday 19/12/25 45 52 W 43 54 N.*' Often the ship would report leaving or arriving in a port. This would replace the longitude and latitude coordinates. The signals officer on the merchant ship would encipher the message, and send it in Morse code to London. The B-Dienst listening stations would then have a three-word 'crib' into the code: the words 'Sirius', 'position' and 'report', which were used every day. Cross-referencing these with the names of dozens of other merchant vessels sending in position reports every day gave Tranow and his colleagues sufficient material to begin reading into the Merchant Ships Code. And given that there were an estimated 3,200 British merchant ships afloat in 1924, there were ample available signals.

The Royal Navy's signals were considerably more complex. The Government Telegraph Code used five-figure groups. The codebook was like a dictionary, where each word – frigate, for example – had an equivalent five-figure group, say 63399. This was enciphered on a subtractor table. For example, the light cruiser HMS *Worcester* would give a daily position report in which its name and coordinates would be translated into groups of numbers. But Tranow knew that one key factor would help him and the team of cryptographers at the B-Dienst. The agents based in foreign ports would tell them the names of the British warships which had docked in, say, Alexandria or Piraeus or Tangiers. So Tranow would have at least two word 'cribs' into the code – the name of the ship, and the name or position coordinates of the port. By following the movements and position reports of British naval vessels across the globe, Tranow knew that however often the letter key changed, or a different subtractor table was used, the B-Dienst would have two letter-group 'constants' for each ship's messages: its name and its daily position. He was further helped by the fact that there were dozens of British naval vessels reporting their position every day.

The next thing that the B-Dienst decided they wanted was a secure means of communication. They needed to be able to send messages to each of the battleships and cruisers in the new German navy, whether at sea or in port. They also needed to be able to communicate with their headquarters in

Berlin. So why not, thought Tranow, simply purchase the Enigma system? The B-Dienst's budget would be able to cover the initial costs required to purchase, say, twenty Enigma machines. And if not, a select group of senior officers and civilian employees in the Reichsmarine knew that additional 'non-official' funds were available for special projects linked to naval rearmament. In late 1924, the German navy contacted Arthur Scherbius once more. Would he, they asked, be in a position to supply them with a number of examples of his rotor machine?

---

* This was the equivalent of £16,000 or $20,000 in 2017.

† The story of Helmut Ruge continues in Chapter 6.

‡ After the outbreak of war in 1939, the code was changed and renamed to reflect the multinational nature of the merchant marine now involved, and became the British and Allied Merchant Ships Code, or BAMS. References to the British Merchant Ships Code still continued in documents and signals.

Chapter Three

GERMANY'S NEW CODEBREAKERS

Wilhelm Fenner freely admitted that when he first began work as a cryptographer he had not the faintest idea of what he was doing. But from an early age he had a keen appetite for order, clearly defined structure and methodical procedure. He was born and brought up in St Petersburg at the end of the nineteenth century, where his father was the editor of a German-language newspaper; and Fenner was the sixth of seven children. His upbringing was strict and governed by the annual rhythms of the Lutheran Evangelical Church; his father tutored him at home for two years and then he spent ten years at a German expatriate Lutheran high school. When he moved to Berlin in 1910 to study construction engineering he joined a fraternity group. The student societies to which most of his fellow students belonged sometimes resorted to duelling to settle arguments or matters of honour. Fenner, however, joined an Evangelical fraternity that forbade its members from fighting. But lack of experience with a sabre did not prevent him from doing well in the disciplines of public hygiene and metallurgy, and graduating from high school as a trainee engineer.

When war broke out in 1914, Siemens gave him a job, while he waited to be called up to serve in a regiment that he thought suited his abilities well. It was a unit that guarded stations, railway property, railways and railway sidings. His dutiful and unremarkable career was then suddenly interrupted for two reasons: Germany was at war with Russia, and Fenner spoke Russian.

From then on it was the geography of his birth, rather than the nature of his upbringing, that decided where his life would lead. He fought for a year on the front line in the snows and on the granite peaks of the Tyrolean Alps, and in Serbia and Russia with an Alpine unit, and then worked at army headquarters as a Russian interpreter, questioning prisoners. Many of the starving men he interrogated in Russian, and its linguistic cousin Serbo-Croat, freely admitted that they had allowed themselves to be taken prisoner simply so they could have something to eat. Commissioned as a lieutenant in 1917, he remained in the army reserves until 1920, when he was discharged. Fenner's Russian language skills had improved, and so with the war over, he avoided the mass unemployment that heralded the first years of the German Weimar Republic. He accepted an editor's job in a fledgling press agency in Berlin run by a Russian officer; this officer in turn introduced Fenner to a former captain in the Imperial Russian Navy, called Piotr Fedor Novopaschenny. The latter had worked as a naval cryptanalyst in the war, cracking the codes of the German fleet in the Baltic. He, too, had made use of copied pages of the naval SMS codebook captured in 1914 from the German cruiser *Magdeburg*. Now he wanted to work for the Germans. Could Fenner help him?

Like the navy, the German army had just set up a cryptanalytical unit as part of the headquarters of their new, post-Versailles army. While the army was called the Reichswehr, the new codebreaking unit was simply called the Cipher Bureau, and came under the Inspectorate of Signals Troops. The first staff members were all civilians, although several of them had served in the army in the preceding war. Fenner approached the head of the bureau, a German army lieutenant, and both he and Novopaschenny were given jobs. They were immediately put to work trying to decrypt telegrams sent to and from the military attaché at the Russian embassy in Berlin. Moscow was, by now, fighting Poland in a small but vicious conflict on the steppes and in the forests on the two countries' joint frontier. Russia wanted to know two things. Firstly, if Germany would take sides, and secondly, how fast it was rearming and with what technology. Novopaschenny taught Fenner everything he knew – the latter freely admitted that until he watched the Russian at work he had absolutely no idea of the basics of cryptography. Cryptanalysis and encipherment, he said, were still naïve and in their infancy. But he learned fast. Within seven weeks he and Novopaschenny were reading Moscow's telegrams, based upon a simple substitution code.[1]

By 1922, Fenner had ten colleagues in his department, which handled cryptanalysis, nine of them men and one woman. Six of them worked on Russian codes, one on Italian, one on French and two on English, with the remaining staff member being a statistician. Among them there was a Russian Jew, a Spanish Jew, a German Jew and a Polish Jew. English, French and Italian codes proved equally easy to crack, as they were also based upon monoalphabetic substitution tables. French newspapers made things easier for them, too: every day they normally published an article loosely based on the information they received from the French embassy in Berlin, which turned out to be much the same information contained in the telegrams Fenner's colleague was decrypting. Life in the department was calm: everybody, Fenner included, was exhausted by five years of war and saw no particular urgency about the work they were doing, even though neighbouring Russia and Poland were fighting each other. They decoded three or four diplomatic cables each day. The terms of the Treaty of Versailles had prohibited the existence of any military or naval intelligence agencies, so Fenner and his colleagues worked at Novopaschenny's private house. Life continued at a sedate pace, and Fenner started a family, marrying, on 11 January 1922, Elise Sophie Katharine von Blanckensee, daughter of Prussian Major General Peter von Blanckensee. They had two children: a son, Siegwart Heinrich born on 28 January 1923, and then five years later a daughter, Ilse, born in July 1928.

By autumn 1924 Fenner had become the director of the cryptanalysis section, and so from then on he went through all the German military's back reports from World War I, as well as reports in the German army library. The new enemy on their eastern front – Poland – added to their workload. Fenner continued to try to recruit staff who were, like him, committed religious men who tended to shun politics. The Foreign Office became suspicious of what he was doing, and, concerned that this new military agency was encroaching on their affairs, said that diplomatic cables were not the business of soldiers. Fenner, however, protested, said they were, and won. A Hungarian and a Pole subsequently joined his team. By 1926 he was reading Polish army systems, Czech army systems and Romanian codes, and realized that once the hurdle of language was overcome, the codes he was dealing with were mainly a matter of simple monoalphabetic substitution. To his natural liking for administration, Fenner now added languages, as the two, he said, were very similar. Things were either right or wrong, in order, or not. As a sign of his character, the first regulation he implemented in his department concerned

the grammatical rules to be used by translators; as a result of this, he got a reputation among his fellow staff as being rather pedantic.

As his agency started to expand, army headquarters told him that his work would now be confined to the cryptographic systems of foreign armies, while a new agency would handle diplomatic traffic. This unit was called Personalabteilung-Z of the Auslandsamt, or Department-Z of the Foreign Service. For ease it was abbreviated to Pers-Z. Shortly afterwards in 1928, Fenner was told that his own cipher department would be equipped with a new communications device for sending signals to army units and the Ministry of Defence. He would personally be in charge of carrying out trials on it. It was, he was told, called the Enigma machine.

But while complex cryptology was constantly developing, the world around Fenner and his men was also changing. Germany was not only struggling to bring itself out of its economic doldrums, it was building relationships with its neighbours. In 1922, Germany signed a treaty of allegiance with the fledgling Soviet Union: this allowed Germany to train military personnel in exchange for giving Russia military technology. Of course, this was against the Treaty of Versailles, which was extremely specific about the permissible details of Germany's military capability. In a dark suggestion of things to come, the German foreign minister who signed the treaty with Russia was killed two months later by two nationalist German army officers, incensed, they said, by witnessing their country attempting to build relations with a communist state. The minister in question, Walter Rathenau, was Jewish. The right wing in Germany continued to grow. In 1923, a political party called the NSDAP, or National Socialist German Workers' Party, emerged in Bavaria, led by a disaffected former army corporal called Adolf Hitler. It was called the Nazi Party for short. Its members staged a small political coup in 1923 in Munich, which became known as the Beer Hall Putsch, or the Munich Putsch. The 'putsch' itself was dramatic. On 8 November 1923, members of the party, who had made a pact with the former wartime general Erich Ludendorff, took over a meeting that the Bavarian prime minister was staging at a beer hall. Both Hitler and Ludendorff declared that the Weimar government was deposed and that they were planning to take control of Munich the following day, helped by 3,000 armed men, but the Bavarian authorities stopped them. Hitler was arrested and sentenced to five years in prison for high treason. He was to serve less than eight months, living in some comfort, and was released just before Christmas in 1924. While he was

in prison, he dictated *Mein Kampf*, which he saw as the backbone to his future ideas and governmental policies. And seeing that armed rebellion was premature, he decided to expend his efforts on legal political ways of coming to power.

Meanwhile, amidst this political turmoil, while the B-Dienst and the German army's cryptanalytical bureau were expanding, so the country was still covertly rearming using the unofficial funding from the Lohmann project. As prototype submarines were being developed Lohmann, who saw himself as a committed German nationalist and patriot, also continued to work on aircraft development, subsidizing the Heinkel, Dornier and Rohrbach aircraft manufacturing companies. In 1926 he even purchased a commercial company called Caspar Aircraft, so that he could obtain facilities for the testing of commercial aircraft which, naturally, bore considerable similarity to the fighter, bomber and reconnaissance planes that were being built abroad by such firms as Boeing, Vickers and Douglas. By 1927 Germany was making excellent progress and had built several successful prototypes. Dornier in Switzerland were about to build a prototype of a huge flying boat with twelve engines, meant to be capable of landing and refuelling at sea, and at the same time, with funding from Lohmann, a project to train pilots was begun. While the rearmament programme he oversaw concentrated on ships, aircraft and submarine design, covert funds from the project also went to equipping both the fledgling Reichswehr's cryptanalytical bureau and the navy's B-Dienst. The latter was, in its early years, from 1922 to 1928, run almost exclusively by black funds. The purchase of Enigma machines from Scherbius and his company's subsidiaries would have been impossible otherwise. Similarly, given that Germany was forbidden to have any form of intelligence services, the provision of expensive and ground-breaking communication equipment could only have come from illegal, treaty-busting sources.

The military, naval and aviation projects that were in development by the mid-1920s included the marine intelligence service, and the submarine being built in Spain, with its bubble-free torpedo tube. Heinkel, Dornier and two other companies were building aeroplanes, in cooperation with the Caspar factory, while the navy was looking at seaplanes and training pilots, and the B-Dienst was expanding. There were torpedo boats too, known as E-boats, and a covert monitoring service for the intelligence services, subsidies to naval shipyards and even yachting schools. Then it all went wrong. Lohmann

appears to have decided in about 1926 that along with the funding from the government, he could move into the commercial world. Two of the pilot projects he experimented with were extraordinary: one company was founded to exploit an experimental method of raising sunken ships by surrounding them with ice, and another sought to extract fuel from potatoes. But the most extreme was the Berliner Bacon Company, which began in the spring of 1926. Lohmann wanted to try to prise the lucrative British bacon market away from Denmark by offering Britain a German product that, he said, would find favour with the notoriously choosy British breakfast palate. He was also thinking ahead – the fast refrigerator ships in which he hoped to carry his bacon could also be used in time of war to carry troops. But in 1927, his company went bankrupt. The implications of this for German naval and military codebreaking, and the development of its respective signals agencies, were immediate. It pushed their funding requirements outwards, towards the German government. Although some of the arms limitation clauses of the Versailles Treaty would eventually be relaxed, or ignored, neither Fenner nor Tranow wanted their agencies and their technical and personnel expansion to have any form of attention drawn to them.

The background to Lohmann's downfall came from his involvement with the Phoebus Film Company, which in 1927 was the third-largest producer of films – or motion pictures – in Germany. From 1924 onwards Lohmann had been giving money to this firm on the specific condition that it produced films of a 'national character designed to stimulate the fatherland consciousness of the German people'.[2] What was also much more pertinent to Germany's expanding intelligence and cryptographical capability was that Lohmann wanted to use the film company and its overseas offices to establish an intelligence network in former enemy countries where Germany was not allowed a naval attaché. There appear to be no reports that he used any of the so-called 'black' funds for his own personal use, or furtherance. Yet what is certain is that between 1924 and 1927 he provided Phoebus, a company capitalized at approximately $1,000,000, with a total of over $2,500,000 of extra funds:

> of only one of five separate grants, a government-guaranteed loan from the Girocentral Bank in Berlin in March 1926. In order to obtain their signatures on this guarantee, Lohmann came up with a plan, informing them that the Lignose Company, a producer of raw film, had also

> guaranteed the loan and that in the event of default it would stand the loss instead of the government. In the early half of 1927 he arranged two more government-guaranteed loans which he kept secret from his superiors by affixing his own signature in the name of the Third Reich.[3]

Despite this massive aid, Phoebus continued to lose money. In 1927 it was in such serious financial doldrums that it failed to meet for its regular annual stockholders' meeting or even to issue an annual financial report. By August disaster was in the air for both Lohmann and Phoebus. The company was falling behind on the repayments on its loans, and penalties were mounting rapidly. None of Lohmann's various money-making projects had paid off, and the black funds were nearly finished. Meanwhile Lohmann was now having his unofficial funding withdrawn by the German government, which they were now channelling elsewhere. Exposure, when it came, was fast. A financial writer on the *Berliner Tageblatt* newspaper had been investigating the state of the German film industry. He could see that the ailing Phoebus was being externally supported – somehow – and when one of the company's former directors resigned, he gave the story to the newspaper. Lohmann, curiously, survived the ensuing scandal, which led to the resignation of Germany's defence minister in 1927.

•••

In 1925, a German army officer called Hans-Thilo Schmidt left the military, no longer able to carry out normal daily duties because of lung injuries sustained in the war from inhaling chlorine gas. He had set up a soap factory, but it had gone bust. His brother, Rudolf Schmidt, then managed to get him a job at the Reichswehr's new cipher bureau. In early 1926, Fenner and his colleagues were still assessing the military version of the Enigma machine, and as they were doing so, Schmidt contacted French intelligence and offered to supply them with information about the new machine. His offer was accepted by one Captain Gustave Bertrand of French intelligence, who gave him the French codename 'Asché', and a contact, the French agent codenamed 'Rex'. For the next several years, until he left his position in Germany, Schmidt met with French agents at various European cities and supplied them with copies of the Enigma machine's instruction manual, operating procedures, and lists of key settings. Even with this information, however, French intelligence were

unable to break messages encrypted on the Enigma. Nor were the British cryptologists whom Bertrand contacted able to make any headway either.

Then on 15 July 1928, the German army and the navy decided to adopt the Enigma. On the same day, Polish codebreakers who had been trying – in vain – to break into Fenner's coding system saw a very distinct alteration in the way German cryptograms were laid out. The previous system had simply taken existing letters in the German language and shuffled them about at random, but this new system appeared to be substituting random letters for vowels and consonants, instead of vowel for vowel and consonant for consonant. The Germans had started encrypting messages using the Enigma. Not only were the Poles already working on Enigma encryptions of their own, they possibly knew from Arthur Scherbius' attempts to sell it to them that the Germans had purchased it. They had also received an Enigma machine themselves by a curious and unexpected route.

The Warsaw Customs Office received a parcel from Germany in late 1927, or early 1928, that stated, on the customs declaration form, that it contained radio equipment. The sales representative of the German firm insisted that the parcel should be returned to Germany without going through customs, because there had been a mistake, and the package should not even have been posted. Because he repeated these demands, the customs officials got in touch with the Polish General Staff's cipher bureau, who opened the package, found that it contained not radio equipment, but an encryption device, examined it, put it back in the box and returned it. It is not known if it had come from Arthur Scherbius himself.

On 15 July 1928 the first German Enigma-enciphered messages were broadcast by German military radio stations; Polish monitoring stations began intercepting them, and cryptologists in the new Polish cipher bureau's German section were told to try to read them. Initially, however, the effort was fruitless. The French, meanwhile, unable to do anything with the Enigma information that Hans-Thilo Schmidt was selling them, decided that it was better off in the hands of one of their enemy's enemies – so they gave it to the Poles. One of the Polish mathematicians, Marian Rejewski, then realized that one of the secrets of the Enigma was that, even if the enemy were given a physical copy of the machine, he would not be able to crack messages enciphered on it quickly enough for it to be of use. What the Poles now had to do was to try to find out the daily key settings for the machine, and they succeeded in doing this because they took advantage of a technique used by

the Germans which they thought gave them greater security. The sender of the message would add on a double repetition of the key to be used so that the receiver did not make any errors. So at the start of each message they would add on three letters – say, HTR – twice. These six letters – HTR – were then put into the daily cipher code on a setting of the Enigma's rotors that was decided between the sender and recipient. As a result, the Poles now had two sets of letters which repeated themselves, giving them a daily crib into the setting of the Enigma machine. This meant that, after lengthy exercises in numeric permutations, they managed to read one Enigma message on the same day that it was sent. In December 1932, Marian Rejewski succeeded in breaking the German armed forces' Enigma machine ciphers, and during the 1930s, he and his colleagues continued to do this, but were extremely careful not to alert the Germans in any way to what they had achieved. They told nobody. Neither the French nor the British. And the Germans did not guess.[4]

Chapter Four

PREPARING FOR WAR

Adolf Hitler became German chancellor in 1933, and in 1935 a unified German armed forces was created. It was called the Wehrmacht, and incorporated the Heer, or army, the Kriegsmarine, and the fledgling Luftwaffe. A paramilitary organization called the Schutzstaffel, or 'Protection Squadron' also existed, founded originally as security bodyguards for the Nazi Party. Out of this the SS grew from a few hundred loyal troops to become one of the main security bodies of the new Germany, and was divided into two constituent parts, the Allgemeine-SS, or General-SS, and the Waffen-SS, its armed units which were established in March 1933. Each of these parts of the new German armed forces was to develop its own signals intelligence agencies, each with a cryptanalytical section. The old Reichswehr was abolished, and a new name was given to the signals intelligence department of the Army High Command, or Oberkommando der Wehrmacht. The agency in which Wilhelm Fenner worked was thus called the Oberkommando der Wehrmacht Chiffrierabteilung, shortened to OKW-Chi.

By now, Fenner had also gained an unexpected ally, in a man called Kurt Richard Selchow who was another Evangelical Protestant, and a former army officer from Upper Silesia who had served in a signals regiment in World War I. He was six foot two inches tall, thin, and had grey-blue eyes. He came from a traditional background, and his father had been a Post Office director in his home town. He had seen in the war that a lot of the work being done by the

German army's signals regiments was in fact diplomatic cable traffic, and so he informed his superiors that a new diplomatic cipher bureau should be established. They didn't listen. Directly after the war ended, he went to work for the Ministry of Foreign Affairs. He worked at the ministry's fledgling cipher bureau, Pers-Z, and recruited men with whom he had served during the war. By the early 1930s, Selchow was the head of cryptography of Pers-Z.

Both Fenner and Selchow wanted to keep their respective agencies free from National Socialist politics. But this proved impossible. By the early 1930s, a selection of increasingly aggressive and forthright Nazi Party members were now working in both Pers-Z and OKW-Chi. In 1933 another new cipher bureau was created by cabinet minister Hermann Göring, a former World War I fighter pilot who became head of the Luftwaffe in 1935. His new agency was called the Forschungsamt, or Research Bureau, and was, on paper, part of the German air force, although it existed primarily to serve Göring and his Nazi entourage's personal appetitite for intelligence. The Luftwaffe would go on to establish another, much larger signals intelligence agency in due course. Nazi party members started leaving the other diplomatic, naval and army codebreaking organizations – Pers-Z, B-Dienst, and OKW-Chi – to join it. They brought their institutional resentments and jealousies of Fenner, Selchow and Tranow with them; they were bitter about the latters' talents and academic successes, and deeply suspicious of their religious, apolitical stance and their refusal to join the National Socialist Party. The seeds of covert resistance to the Third Reich were being sown. As Wilhelm Fenner later said:

> OKW-Chi was engaged in a war against an as yet unknown number of 'foreign' foes whose weapons were their cryptographic systems: the 'inner foe' which caused far more vexation was Göring's agency. It is true, I was still in a position to hire people who as a rule had not yet left the church, and were not in the NSDAP, but a certain letting down of what we may term 'attitude' was present.[1]

Both Fenner and particularly Kurt Selchow were protected by the anti-Nazi Klaus von Bülow, who was secretary of foreign affairs. He opposed the National Socialist Party, and was adamant that all diplomatic signals traffic, and the enciphering and decrypting thereof, should remain the preserve of Pers-Z. Selchow, seeing the way the political wind was blowing, offered his

resignation to Von Bülow in 1934, but was persuaded to remain. The foreign minister was keen not only that Pers-Z should remain separate from the political influence of the Nazi Party, but that it should be staffed by people who were firmly opposed to its principles. This was dangerous ground. But as long as Von Bülow was in position, Selchow, and by extension Fenner, were protected.

However, in 1938 Von Bülow died, and Joachim von Ribbentrop took over. An ardent National Socialist, he tried to transfer as much practical knowledge, talented personnel and influence over codebreaking away from the army, the foreign ministry and the navy to the Luftwaffe and the SS. Fenner found himself in a very fragile and dangerous position. On one occasion he was accused of being a Jewish sympathizer because he wouldn't participate in nocturnal 'Jew raids' with the Nazis in his department. A colleague from the SS was later to say that he had been overheard making disparaging remarks about the Sicherheitsdienst, or SD, which was the newly created intelligence service of the SS. The National Socialists in his office would offer round Nazi Party cigarettes; a refusal to accept one was deemed sufficient proof of where a person's political sympathies lay. Fenner's telephone at work was tapped. And in this minefield of political loyalty, Kurt Selchow then went one step further in his stand against National Socialism. Göring's Research Bureau started trying to remove key codebreaking tasks from Pers-Z, in a bid to increase the power that Göring held in the Reich's intelligence community. Selchow and his staff were ordered to share all of the information they gathered from breaking and reading any British, French, Russian, Italian and Swiss diplomatic codes. Selchow started falsifying some of the information he had gathered. He passed the fake information to Göring's Luftwaffe bureau, who in turn passed it to the SS. Meanwhile, in this atmosphere of mutual suspicion between the Third Reich's Nazi leadership and the talented cryptanalysts from the army, navy and Foreign Office, war was coming closer.

German Signals Intelligence Agencies from 1938

The respective signals intelligence agencies and their cryptanalytical units were also growing in size. By 1938, there were ten different formations who were dedicated to intercepting, monitoring, deciphering and reading the codes both of Germany's enemies, inside and outside the Reich, and of

neutral countries. They would remain the same throughout the whole of World War II, with the only changes being in the number of persons they employed, and the relative successes and failures of their battles in the war of codes. They were as follows:

i. The first signals intelligence service was a non-covert, bureaucratic and very normal organization – the Deutsche Reichspost, or German Post Office, and its job involved intercepting and reading key telegrams that passed through its offices, sent by foreign companies and individuals living within Germany's borders. The Post Office's Forschungsstelle, or Research Bureau, also provided interception services on any phone calls that were made on telephone lines registered with the German Post Office.
ii. The second agency was the Forschungsamt, Hermann Göring's Research Office, which was not part of the Luftwaffe, simply overseen by him.
iii. Third came Kurt Selchow's unit at the ministry for foreign affairs, Pers-Z.
iv. Fourth was Wilhelm Fenner and the OKW-Chi, the Oberkommando der Wehrmacht's Chiffrierabteilung, the Wehrmacht High Command's decryption department.
v. The fifth unit was two sub-agencies run by the Oberkommando des Heeres, or OKH. These were respectively the Abteilung Fremde Heere Ost (Department for Foreign Armies East), the intelligence department focusing on the armies of eastern countries such as Russia and Poland; and the Abteilung Fremde Heere West (Department for Foreign Armies West), which focused on the military forces of countries to the west of Germany, like France, Spain and Britain.
vi. Next in line was the in-house decryption service run by the Oberkommando der Wehrmacht (OKW) counter-intelligence service, known as the Abwehr.
vii. Agency number seven was the Luftnachrichtenabteilung of the OKL, the Oberkommando der Luftwaffe. This agency, for short, was called OKL Chi-Stelle.
viii. Eighth was the crucial Beobachtungsdienst, the B-Dienst of the Oberkommando der Marine, or OKM, Wilhelm Tranow's naval codebreakers.

ix. Next came the decryption and monitoring service run by the Third Reich's institutional security apparatus, the Reichssicherheitshauptamt – Reich Security Main Office, or RSHA. This was overseen by the SS.
x. Lastly came the OKW-GdNA. This stood for Oberkommando des Heeres/General der Nachrichtenaufklärung, and was the overall signals intelligence agency of the German regular army before and during World War II. At the outbreak of war, it assumed some of responsibilities for military signals intelligence and cryptanalysis from OKW-Chi, and from 1940 it was simply known as Inspectorate 7/VI. It was the parent organization of the two OKW groups for eastern and western armies mentioned above. Only after the failed plot of 20 July 1944 against Hitler did it become known as the GdNA. Although a lot of its work duplicated that of OKW-Chi, it was essentially the main regular army signals intelligence and cryptanalysis unit, working on both Western and Eastern Fronts, as well as in the Mediterranean.

The codebreaking agencies of the Third Reich were born and raised on solid and bureaucratic Teutonic organization and administration. At the beginning of the 1930s Wilhelm Fenner thought that OKW-Chi should be an umbrella agency for all the others, and that one single codebreaking 'clearing house' should exist, where all information was shared. No such thing was to happen. Instead, although the organization of each agency was a model of administrative performance, the relationship between them was sometimes the opposite. They veered between cooperative co-existence to distrusting each other, being jealous of each other, and refusing to share information or indulging in petty inter-departmental rivalries. The academics thought the soldiers were Prussian and inflexible. The soldiers thought the scientists were ill-disciplined with no respect for the traditional ways of doing things. But the fundamental disagreements between both sides focused on support, or the lack of it, for the National Socialist Party. As would become apparent, this severely damaged the operational efficiency of Germany's cryptanalytical capacity. The situation was often compounded by the climate of suspicion and fear that was the running fuel of the Third Reich, where there was little or no effective filter between the paranoid fears of its leader, Adolf Hitler, and the decisions that his senior generals and admirals had to implement. This sometimes meant that however good was the intelligence gathered by Germany's codebreaking experts, implementing it operationally was another

matter.

To understand what each agency did, it is first necessary to see how they were organized. The two largest were OKW-Chi and the B-Dienst,* and both were organized along similar lines. The system of monitoring stations that both had set up, and used, also shared their information with the other smaller agencies. OKW-Chi, being an armed forces agency, also shared its monitoring facilities and gathered information with the Abwehr, and with the two signals intelligence departments that worked for the Heer against the armies of both eastern and western countries.

OKW-Chi had two separate monitoring systems based upon a network of intercept stations. The three main ones were firstly at Lauf, in western Baden-Württemberg, on the edge of the Black Forest. Set in a valley that sloped east to west, the town was close to both the French and Swiss borders, and made it easier to intercept the signals of both nations. The second station was at Treuenbrietzen, roughly fifteen miles south-west of Berlin's outer suburbs, with the third at Lorrach, a chocolate-making town just north of Basel at the intersection of the French, Swiss and German borders. Each station had a number of intercept 'sets' – radio antennas and aerials that picked up the signals sent in Morse code by the armies, police services, foreign ministries, air forces and navies of the countries like France or Switzerland to whom the Third Reich was listening. By the outbreak of war, nearly 180 people worked at Lauf. Subsidiary to the three main stations in Germany, there were two additional 'out stations' in Spain and Bulgaria, run by the Abwehr.

The Spanish out station employed around thirty-five people in 1939. At first, it was established in the German consulate in Madrid, with sub-stations established; one on a cattle ranch north of Seville, one in Tangiers and one in the Canary Islands. The Spanish government of General Franco officially approved of the work of the German out stations. The Germans made extensive efforts to keep their network of out stations secret, but the Spanish intelligence services were continually keeping them under observation. The German personnel wore civilian clothes and were formally forbidden to mix with Spaniards; they had to travel in small groups, married men were not allowed to contact their wives, and single men were not allowed to marry Spanish women. There were other out stations in Rome, Belgrade, Vienna and Budapest, and after the outbreak of war these were obviously expanded into countries occupied by the Germans.

The military head of OKW-Chi was then an army colonel, and each

month he and Wilhelm Fenner would make an appraisal of the most interesting information picked up by each listening station. The operational centre of OKW-Chi, meanwhile, was the cryptologic bureau, which was commanded by Lieutenant Colonel Fritz Boetzel, with a major as his deputy. Before the outbreak of war, the two army officers would make a number of trips from the listening stations at Lauf and Lorrach into neutral Switzerland, where they were in contact with a group of Russian émigrés. Neither man suspected that German colleagues from the Abwehr might be watching them. But they were.[†]

Meanwhile, on the eve of war OKW-Chi was organized into three main groups, A, B and X, with overall command from the military. Wilhelm Fenner held the rank of a senior civil servant, and headed the cryptographic bureau. Group A's main task was inventing their own cryptographic systems, as well as intercepting foreign radios and cables. Group B focused on the cryptanalysis of foreign government communications, and the development of the mechanical cryptanalysis devices including training in such devices. Group X scanned and forwarded deciphered telegrams to various departments in the army and the Foreign Office. Within the different groups were sub-sections known as *Referate*. The different responsibilities for each of these sub-sections covered every possible eventuality in codebreaking: inventing ways of disguising German telephone and radio communications, preparing code and cipher manuals, overseeing the internal security of the organization and investigating lost equipment. In the unthinkable event, for instance, that somebody within the Abwehr or Army High Command – or the troops in the field – were to lose an Enigma machine, the section Referat IIa would be the one to investigate. Sections IIb and IIc invented codes and ciphers and managed the cryptological needs of Abwehr agents operating in the field. Another sub-section monitored the foreign media and their propaganda transmissions.

This administrative and operational protective circle surrounded the heart of OKW-Chi. The department called Chi IV, which was the codebreaking and translation service, took incoming signals from the network of intercept stations, translated them and broke the codes in which they were decrypted. From 1939 onwards this department was overseen by Fenner, but headed by a senior mathematician who had joined OKW-Chi in 1937. His name was Dr Erich Hüttenhain, and he was a former astronomer who had specialized in Mayan history. He too was religious, and was the son of a Protestant priest.

When he joined OKW-Chi, he met Wilhelm Fenner. The latter, interested by his knowledge of Mayan history and signs, gave him a test. He sent him a message which had been encoded with a private cipher. Hüttenhain duly deciphered it and was accepted as a possible codebreaker, and at OKW-Chi he was employed as a specialist who was given the responsibility of building a cryptanalytic research unit, a group that would identify, investigate and attack enemy coding systems.

Hüttenhain was accompanied by a loyal assistant called Dr Walter Fricke, a well-known astronomer, to whom he told everything he knew. The latter was methodical, dutiful, precise, and saw and heard everything; he was considered the official historian of the organization, so he conscientiously documented the changes and developments in it. But he was also keeping records in another way. The security regulations of the Wehrmacht High Command specifically forbade soldiers and civilians from taking official operational information, such as the details of cryptological developments, and making private records of them. But unknown to all his colleagues, apart from Hüttenhain, Fricke was keeping a private diary.

The section headed up by Hüttenhain was predominantly made up of mathematicians. The principal job was to break into enemy ciphers, and establish and recognize the code in which each was written. Once decoded, the actual translation of the signal from English or Italian or Turkish was handled by one of the department's linguists. Outside of the section devoted to cryptanalysis, other departments handled the running of the expanding networks of listening stations and out stations, were responsible for the radio monitoring, looked after the radio equipment, ran the personnel department and managed the carefully coded and organized card system. Every time a foreign military or diplomatic signal was broken, the salient details from it – people's names, places, army units, times, code words – were entered onto cards which were then stored in a filing system.

A German scientist called Dr Franz Weisser joined OKW-Chi in 1936. He had wanted to be a schoolteacher but could not get a job because he was not a member of the Nazi Party, so he joined the Wehrmacht as a civilian employee. He worked in the section dealing with the decryption of American and British codes. There were fifty men in the decryption sections in the second half of the 1930s, but, Weisser later said, the actual work was done by five people, himself included. He remembered the working atmosphere, and the character of Wilhelm Fenner:

> Fenner was a very difficult character. He knew the fundamentals of the old school cryptography and was a good organiser. Some say he was an intriguer. To people whom he liked he was frank and kind, to others he was very cunning – a diplomat. Fenner was very susceptible to flattery and a pleasant way. A confirmed Protestant and an anti-Nazi. When I joined OKW-Chi Fenner told me that the official greeting might be 'Heil Hitler' but in OKW-Chi only 'Good morning' was used. Fenner had much trouble because he was an anti-Nazi.[2]

While the cryptanalysts at the Wehrmacht High Command were busy expanding their organization, and balancing the operational demands of their job with treading the tortuous political path of Nazi Party politics, the codebreakers at Pers-Z, the Foreign Office, were busy as well. Their cryptanalysts were in charge of decryption of the diplomatic codes of Ireland, Spain, Great Britain and Portugal. Everybody could see war was coming – but by constant monitoring of diplomatic signals Pers-Z could see that nobody, apart from Germany, knew when and how. They read signals that described the intricate posturing of various national governments in the lead-up to war. Who would fight with or against Germany? Who would remain neutral? What would the Japanese do? The Gestapo and the Abwehr had embarked on a programme of burglary, and attempted theft or copying of signals codebooks from government ministry buildings in such cities as Rome, Paris, Prague and Madrid. German signals intelligence staff from the Wehrmacht High Command, OKW-Chi, were now helping Franco in the Spanish Civil War, as were the Luftwaffe's signals intelligence teams. The Kriegsmarine had set up two listening posts on the Spanish coast, and the B-Dienst had by now begun to break two of the Royal Navy's main codes. Wilhelm Canaris, by now a vice admiral, had been made head of the Abwehr in January 1935 and was trying to persuade Franco to join the forthcoming war. The Germans even considered a potential plan, codenamed Operation *Felix*, to seize Gibraltar, but this was dependent on Franco entering the war on the German side. Unbeknown to Canaris, Heinrich Himmler, who was the head of the SS, and Reinhard Heydrich, the head of the SD intelligence service, did not trust him, so both the Luftwaffe and the Wehrmacht High Command signals intelligence services were ordered to try to gather intelligence on his activities in Spain. The Third Reich was listening to its own.

Ferdinand Feichtner was an only child from Bavaria, who had dropped out of high school so he could concentrate on becoming an electrical technician.[3] In 1922, when he was only fourteen, he began an apprenticeship, attended on-the-job training at an electro-technical school in Bavaria, passed the exams to become a licensed electrician, and then joined the army when he was eighteen. His grandfather had been a soldier, as had many of his relatives, and for the technically minded Feichtner, obsessed by things electronic, the camaraderie and team spirit of the army appealed to him. He was posted to a signals unit outside Munich, and his non-commissioned officers immediately saw his potential. He was brusque and could be anti-social, but put him in front of a radio set and he could coax signals out of the ether.

In 1929, when he was posted to a signals intercept station in Bavaria, he found his métier. His job was sitting in a monitoring station trying to pick up the coded diplomatic signals, sent in Morse code, of the Swiss, French and Italian governments, coming from Bern, Lyon and Milan. He became expert in radio direction-finding: triangulating the incoming beams from three different foreign radio stations, and then working backwards to find out where these stations were geographically located. He passed his NCO course, became a sergeant, and by 1930 was in charge of a small unit that reconnoitred the border area with Switzerland for suitable mountain locations where they could install intercept units. Incoming signals were at their clearest the higher Feichtner climbed, he found, and one day in the Bavarian Alps he discovered he could pick up radio traffic from Africa.

By 1935, Adolf Hitler had come to power, and Feichtner, like many others in the newly established Wehrmacht, found his patriotism and nationalism appealing. He also liked the fact that Hitler was not from a landed Prussian family, but from a simple background, and had himself been a junior NCO. The shadow of the SS and the SD hadn't yet cast its moral and political darkness over the life of those like Staff Sergeant Feichtner in the early 1930s: he was too busy getting promoted, and teaching civil servants about radio communication so that they could take their place in the newly established Luftwaffe officer cadres. He had little time for these men, whom he saw as self-serving bureaucrats more interested in having an easy job than in learning about the technology that might one day stand their air force in good practical stead. So in 1937, when he found his perfect radio intercept location

at 4,000 feet up a Bavarian Alp above Wendelstein, he managed to get himself posted there for a year. The crackling blips and dashes and dots and whirrs that swirled around his intercept station in the Alpine sky were not, he discovered, coming from Italy or France: to his surprise, he found they were coming from Spain.

The Civil War there was at its height, and Germany was assisting the regime of General Francisco Franco. And so in early 1938 Feichtner's commanding officer pulled him down from his Alpine listening post, and sent him to Spain to work with one of the joint German army and air force radio intercept units.

When civil war had broken out in Spain in July 1936, Adolf Hitler had immediately sent air force and army units to assist General Franco and his Nationalist forces. The Soviet Union sent smaller forces to help the Republican government, while Britain and France and two dozen other countries set up an embargo on any munitions or soldiers heading into Spain. Germany also signed the embargo but simply ignored it. The war provided combat experience with the latest technology for the German military, but it also risked escalating into a world war, for which the Germans were not yet prepared. Crucially, the fighting in Spain allowed the Germans to train men and test equipment and tactics. Under the collective name of the Condor Legion, 7,000 Germans started arriving in Spain from July 1936 onwards. At sea, the Maritime Reconnaissance Squadron of the Legion took action against Republican shipping, ports, coastal communications and occasionally inland targets. Then-Captain Karl Dönitz even sent submarines, in a small deployment named after his daughter, Operation *Ursula*.

The tightly disciplined, technically minded Feichtner was astounded by the war in Spain. Where, he thought, was the sense of public morality and common good that ran through daily life in Bavaria like a powerful underground river? His opinions were formed by what he saw around him, and by the conversations he and his German colleagues had with Spanish soldiers. The Republican movement, he surmised, was all over the place. On the one hand, yes, the Spanish peasantry worked hard despite being trodden underfoot by the landed gentry, and there was a strong religious ideal. But Franco had the right idea, he thought. The destiny and dreams of a European country couldn't be decided by somebody who lacked discipline or political will.

The radio discipline and code procedure of the Spanish Republican troops

was so amateur and so shaky, Feichtner found, that he could work out everything he needed from their signals: the order of battle of their troops, where their puny air force took off, and, most importantly, where on the coast their supply ships docked. Freighters bringing arms, volunteers, equipment and food for the Republicans would dock at certain ports on the Mediterranean coast at specific times, unload as fast as possible, and then be out to sea in international waters before the prowling German Heinkel bombers could catch them red-handed. But Feichtner worked out that the Spanish customs offices and harbour masters were sending signals, hamfistedly coded, out to the freighters as they stood off the coast, warning them when the coast was clear to land. The moment Feichtner's unit picked up these messages, they decoded them as fast as they could. Then it was time for the radio message to the airbase of the German Condor Legion, the Messerschmitts and Heinkels that formed Hitler's aerial assistance to Franco. And as a freighter moved in to harbour, inbound from Piraeus or Istanbul or Split and filled with arms or medical supplies for the Republican movement, there would be the sudden dark ravens in the sky of Nazi bombers, and seconds later 500lb bombs dropping from a mere 300 feet onto the cargo boats, moored like sitting ducks. Feichtner's German and Spanish superiors were very impressed; he was made a regimental sergeant-major.

Feichtner's interest in cryptology and encipherment peaked in Spain; he saw immediately what the Republicans were doing wrong. The word sequences in their coded messages never changed, so it was possible to spot distinct patterns in them. The content of the message was always similar – '*freighter Andromeda will be arriving in Valencia on 12/8 at 2300*' – or they gave the times and details of a unit's incoming attack. The 'indicator' of the Republican messages was always put at the beginning, it always consisted of the same number of letters, and the code the Spanish rebel troops used was always the same. In short, thought Feichtner, it was an object lesson in how not to encode and send encrypted messages. Even when the Republicans started changing their codes every month and then every week and then every day, he and his men could still read them within hours.

Then in 1938, his twelve years of military service came to an end. He asked to go back home. He wanted to leave the army and become a civilian, and transfer his knowledge of radio technology to a steady job with the Telefunken company. But the army wouldn't let him leave. Feichtner registered a formal protest. The military personnel department registered his

complaint, told him he could leave, but said that they would be obliged to enter onto his service record that they could not keep him in the army against his will when his twelve years of service was up; but that he had deserted the Fatherland in its hour of utmost need. And that, knew Feichtner, in the Third Reich of late 1930s Germany, was akin to professional and social suicide.

Instead, Feichtner volunteered to become a signals instructor in the Luftwaffe, transferring sideways from the army. He specialized even further, adding two more technical trade certificates to his hard-won wartime experience in Spain, and then the Luftwaffe sent him to their Signals Intelligence School in Munich, and made him an officer.

Shortly before the war broke out, he and four colleagues from the Luftwaffe and Wehrmacht boarded the Zeppelin air balloon codenamed 'Hindenburg'. They were due to be joined by a number of civilian employees from the Luftwaffe who had planned the trip. But Feichtner was not surprised when they did not show up at the Frankfurt airfield from where the Zeppelin took off. None of the five soldiers or airmen were concerned – the mission was quite simple. It involved testing radio direction-finding equipment from a substantial height, to see what they could pick up from the French, Belgians and the British. What was meant to be a technical exercise turned, instead, into a ballooning holiday, drifting in the spring sun over the North Sea coast, looking down on Belgium and France, and across the Channel towards England. Feichtner later remembered it as a moment of idyllic relaxation. The next time he would see France, he would be in the middle of invading it.

•••

The Germans Try to Decrypt Chamberlain's Messages at Munich

Signed on 30 September 1939, the Munich Agreement allowed Nazi Germany to annex parts of Czechoslovakia with a German majority, lying along Germany's south-eastern border – the area known to the Germans as 'the Sudetenland'. Hitler, seeking an excuse to occupy the territory, claimed that the German population in the area was under attack by Czech nationalists. Hungary and Poland both wanted to take parts of Czechslovakia that they insisted were their own territorial property. Italy's dictator Benito

Mussolini backed Hitler, and the issue of the Sudetenland lay like very thin ice over the freezing waters of a lake. Negotiations for the agreement took place in Munich between Germany, France, Great Britain and Italy, but the Soviet Union was not invited. France and Great Britain were caught between trying to prevent another war, and attempting not to be seen to be appeasing Hitler; in the light of this, if guarantees of European territorial security could be respected, they were prepared to allow him to occupy the Sudetenland.

Needless to say, in the run-up to the Munich Agreement, it was of crucial importance to the Germans that they knew Britain's negotiating position, and what its forthcoming course of action would be vis-à-vis France, Poland and Czechslovakia. The Foreign Office's codebreakers from Pers-Z and Göring's Research Bureau were given the task of trying to monitor, intercept and decrypt any messages sent from London to the British embassy in Berlin before, during or after the conference. The Germans also tried to decode French diplomatic communications and listen to the telephone conversations of politicians and diplomats, particularly the Czech President Benes and his ambassador in London. The British bargaining position was clearly being decided prior to the conference amid fast-moving geopolitical events across Europe. British Prime Minister Neville Chamberlain had a meeting with Hitler on 15 September at Berchtesgaden, where the latter made his position clear:

> Three hundred Sudetens have been killed and things of that kind cannot go on; the thing has to be settled at once; I am determined to settle it; I do not care whether there is a world war or not; I am determined to settle it and settle it soon and I am prepared to risk a world war rather than allow this to drag on.[4]

Both sides knew their subsequent courses of action would be decided by what Germany did, rather than what it said. Great Britain desperately needed more time to complete its rearmament programme if war was coming; Germany feared the might of the Royal Navy, and was racing to complete the building and subsequent launching of at least two more capital ships, *Bismarck* and *Tirpitz*. Naval officials told Hitler this would take a minimum of another eighteen months. It stood to reason that Germany's cryptanalysts at the Foreign Office and in Göring's Research Bureau would have been instructed to find out what messages were being transmitted backwards and forwards

between the British government in London and its embassy in Berlin.

> In 1938, during the Munich Conference, the Research Bureau is said to have solved the British system which carried Chamberlain's messages to London. Hitler once delayed a conference with Chamberlain for several hours in order to get some decodes.[5],[‡]

Great Britain's Foreign Office diplomatic code was a five-digit one, enciphered with a codebook containing 40,000 elements, which substituted groups of numbers for words or letters. Yet the period around the Munich Conference was so frenetic in terms of diplomatic wireless activity, that there is a possibility that this normally secure system could have been compromised:

> Of the numerous examples which might be adduced, the following may serve as an example: the additive number used by Great Britain, which ran to 40,000 elements and served for the encipherment of the 5-digit code and was replaced at definite intervals of time, offered as a rule adequate assurance of security. But if in periods of greatly increased diplomatic activity with telegraphic traffic many times the usual volume the additive is not replaced correspondingly sooner, especially since increased security is desirable in such periods, then this is a sign of deficient control.[6]

What this meant was that when Britain's diplomats were busy, as at Munich in 1938, and signals traffic was heavy, then because they didn't replace the means of encryption – the additive – often enough, the Germans could break into their codes. The British Foreign Office made an internal report about the incident:

> Despite an extensive attack in 1938 and 1939, the Germans failed to break the long subtractor system used to re-cypher the Foreign Office's basic cypher books. Against similar tables that were in force from November 1940 to January 1941 they had some limited success, but not enough to enable them to reconstruct the book before both the basic book and the tables were again changed. There is no evidence of later success, and according to German testimony after the war the main

Foreign Office systems were never broken.[7]

The matter was to rest there, at that point. Events swiftly overtook any cryptanalytical movement on the ground, as on 30 September Chamberlain signed the Munich Agreement, and returned to London declaring to the British people that the accord represented 'peace for our time'. Hitler moved in to the Sudetenland the following day. War was now fast approaching.

---

* Due to their size and greater effectiveness, OKW-Chi and B-Dienst form the focus of this work.

† The activities of Boetzel and his deputy in Switzerland are outlined in Chapter 22.

‡ Chamberlain met with Hitler on 15 September in the Alps at Berchtesgaden, on the 22nd, 23rd and 24th in Cologne, and lastly on 29 and 30 September for the signature of the Munich Agreement. If the Germans were reading British diplomatic codes, it seems most logical that any meeting between the British prime minister and the German Führer that was delayed was in Cologne.

Chapter Five

THE KRIEGSMARINE STARTS LISTENING

On 27 January 1939, Hitler ordered the launch of Plan Z, a huge programme of naval expansion designed to build a German fleet that by 1944 would be capable of defeating the Royal Navy. For the first and last time in the Third Reich, the Kriegsmarine was given a priority over all other branches of the armed forces in terms of allocation of resources. The Naval High Command, the Oberkommando der Marine, or OKM, had designed a plan that would include ten battleships and four aircraft carriers, as well as cruisers that would attack British merchant shipping, but only a small number of U-boats. By the time World War II broke out in September 1939, very little work had been done on the new ships commissioned under the plan, and the capital ships that made up, or would be added to, the German navy had all been laid down prior to Plan Z. They were expensive, too: the battleships *Scharnhorst* and *Gneisenau* cost almost 300 billion Reichsmarks, while the *Bismarck* and the *Tirpitz* cost almost the same. These funds could have produced another hundred Type VII-A U-boats, but in September 1939 the OKM was focused on surface warfare. However, one subsidiary effect of Plan Z was that the naval signals intelligence service, the B-Dienst, received considerably more funding. The OKM's strategic thinking was that if its cryptanalysts could use their skills to detect the whereabouts of the Royal Navy's ships, then their surface fleet could find and sink them.

In 1938, before the war started, Wilhelm Tranow and the B-Dienst still

had problems finding sufficiently qualified and suitable personnel for their cryptanalytical department. The staff members who were Jewish, or part-Jewish, had left or been removed. From 1933 to 1934, German legislation at state and national level concentrated on limiting the extent to which Jews could take part in public life. The Law for the Restoration of the Professional Civil Service came in on 7 April 1933, and it decreed that Jewish and 'politically unreliable' civil servants and employees were to be excluded from state service. This new Civil Service Law was the German authorities' first imposition of what was called the Aryan Paragraph, a regulation used to exclude Jews and often other non-Aryans from public life, and various organizations. Civil servants apart, one effect of this new legislation on Germany's signals intelligence services was that Jewish civilian workers were forced to leave the service of the armed forces. This also immediately reduced the number of qualified and well-educated potential cryptanalysts. Young German men were now being recruited, or conscripted, for the Heer, the Kriegsmarine and the Luftwaffe, while the SS was now 90,000 strong.

But by the eve of war, in October 1939, the B-Dienst still had only forty men working in its English section on one of its principal targets, the British Naval Cypher. This encrypted the Royal Navy's operational signals, while the Naval Code encrypted administrative ones. These cryptanalysts concentrated very specifically on the Royal Navy's operations in those areas that interested them most, namely the English Channel, the North Sea and the Atlantic. The main prerequisite for recruits was that they should speak, write and understand any foreign languages. They were then given the standard B-Dienst six-week training course, which focused on Morse code, an understanding of basic cryptology, radio direction-finding, signals and use of teleprinters. Tranow and his team were faced with the enormous task of trying to break into, and continue to break into, the codes of the Royal Navy, but he found he did not have enough personnel to work on all the British codes simultaneously, so he told his best cryptanalysts to concentrate on the Royal Navy's more general Administrative Code, which was a five-figure code reciphered on a subtractor table. Like all the other British maritime codes, this was a cipher based on a codebook.

How the British Royal Navy Enciphered its Radio Traffic

Like the German navy in World War I, one of the basic cryptosystems that

the British Royal Navy used for important radio traffic were codebooks, which were then enciphered using subtractor tables. These codebooks were four-figure ones, and the encipherment with the subtractor tables was carried out using what was known as 'the left to right non-carrying system'. The British naval codebooks did not differ very much from the ones used by the Germans in 1914–18, and were similar in layout and principle to the ones captured from the SMS *Magdeburg* in 1914.

The codebook was in essence a dictionary that assigned a four-figure group to each of thousands of words or word groups, such as destroyer, making smoke, port, starboard and so on. For example, in the book the word 'cruiser' could have the code 3312, 'open fire' 2988, and 'torpedo' 3510. So the first thing that a Royal Navy signalman would have to do was to find the number groups in the codebook that corresponded to the individual words in the message he wanted to send. After this, he would use the subtractor tables to encipher them. What this meant was that the four-figure number corresponding to the word would be subtracted from what were known as the 'key groups' of the subtractor tables. These were other groups of four-figure numbers. In some codebooks the coding and encipherment figures were put together in groups of five numbers, not four, but the principle was exactly the same. A word from the codebook was enciphered by taking the number that represented it in the book, and then subtracting it in a particular way from one particular number in the encipherment table. The particular method in which this was done was that, as illustrated below, the resulting number would not have any of its surplus numbers 'carried over'.

Once the sender of the message had enciphered the words of his message on his subtractor tables, he would put an 'indicator' at the start of the message. This would be another group of numbers. What this told the ship or office to which the signalman was sending the message was which page, and line, of the subtractor tables were being used on that day or week or month to encipher messages. By using this indicator, the recipient of the message would then go to his subtractor tables, find the page and line and word necessary, which would then give him a four- or five-figure number, and from this he would subtract the coded number group he had received in his message: this subtraction, if done correctly, would then result in the number that originally came from the codebook. Having both encipherment tables and codebook to hand, the recipient then simply took this number, checked it in his codebook, and it gave him the original word. It went without saying that this was a

time-consuming process, however fast the radio signalman could operate.

An example would be like this:

The coded message of the day is ***BATTLESHIP SIGHTED NE CRETE***

The code numbers in the Royal Navy book for the four respective words are **5213 9092 1087 3890**

The signalman goes to his Royal Navy Cypher No. 1, and chooses a *random* page and *random* sequence of four-digit numbers from any line. It doesn't matter if they are greater or smaller than the code numbers. The page and line number will be clear from the indicator to the recipient, who has the subtractor tables. So if the enciphering numbers or key groups are as follows:

9193 5264 8129 2005

subtracting the code words from the key groups gives:

5213 6272 7142 9215.

The 'non carrying subtraction' is done as follows:

9193 - 5213 = enciphered word **4980** (from left to right: 5 from 9 is 4, 2 from 11, because 1 is less than 2, is 9, 1 from 9 is 8, 3 from 3 is 0)

5264 - 9092 = 6272 if the subtraction is done without carrying (2 from 4 is 2, 9 from 16, because 6 is less than 9, is 7, 0 from 2 is 2, and 9 from 15 is 6)

8129 - 1087 = 7142

2005 - 3890 = 9215

It is important to subtract one figure at a time, going from left to right, and not to carry, ever. Each number is entirely independent of its neighbour, otherwise there will be ambiguous results. To decipher, the recipient goes to his book of key groups, finds the right page and line, and reads off the four numbers (**9193** etc.). He then subtracts (still without carrying) the enciphered word – **4980** – from the key word in his cipher book – **9193** – to give him the code word **5213**, which he then looks up in the codebook and finds that it means 'battleship'.

So to be able to decrypt and read intercepted Royal Navy codes, and thus to be able to reconstruct their codebooks, what Tranow and his teams needed were all or some of four things. Firstly, 'depth', i.e. as many as possible of the same words or same messages to be repeated; this was something which the Royal Navy did frequently, and which was often unavoidable. For instance, various words or phrases were repeated out of necessity, not only naval terms like port or starboard, but signals that gave the ship's position, ambient weather conditions, whether it was entering port, leaving port, or needed

repairs, the name of the port it was leaving or approaching, the names of the other ships with whom it operated in a squadron or a flotilla, and whether there were submarines or aircraft involved in an exercise with it. These words would provide a constant menu of 'cribs' repeated from one message to another, whose encipherment German codebreakers could use to compare both between different codes and also with messages broadcast in 'clear'. If they discovered a message that was sent both in code and in clear, where they could compare both sets of cipher text and plain text, this was known as a 'parallel text compromise'. The messages that helped cryptanalysts the most were those where the same words or word groups were repeated on a regular basis; this was why such signals as weather reports and messages indicating a ship's position were so useful. It was a matter of looking for consistent variables.

Secondly, it helped the Germans considerably if the Royal Navy failed to change their codebooks for a long time, which the British did, giving the Germans plenty of repeating material to gather, and plenty of time to experiment. Thirdly, it greatly assisted the Germans if their enemy used several different codes and codebooks – for the Royal Navy, Merchant Navy, submarines, convoys etc. – that were all basically the same, with four- or five-figure groups enciphered against subtractor tables. If these were only changed at different times, they gave the Germans repeated cribs from one code into the other. It was to the Royal Navy's detriment that they occasionally managed to do all of these things, all at the same time, from 1934 until 1943.

Yet despite the extra funding available from Plan Z, and the successes Tranow was enjoying against the British naval and merchant codes, by the end of 1938 his staff had only increased by about twenty from the previous year, and the B-Dienst's chief cryptanalyst was finding it increasingly hard to balance the demands of regular, persistent and successful decryption with too few personnel. Had he had more people, he knew, it is highly likely that he would have had more successes earlier on, which would have enabled him to isolate the ships of Britain's surface fleet, and their submarines, faster and more regularly.

As explained, the bedrock of the Royal Navy's main cryptologic systems were codebooks and enciphering tables, which differed only through having four or five numbers with which to represent words. As we have seen, Naval Cypher No. 1 was a four-figure book and the Administrative Code a five-figure book which was used from 1934 till August 1940. There were some

subsidiary codes too, such as the Auxiliary Code No. 3, a four-letter book that was used from 1937 until August 1940 by small units, like Motor Torpedo Boats (MTBs). These were then enciphered with what were called 'Auxiliary Vessels Tables'. What was immediately obvious to Tranow and his men was that these ciphers and codebooks had been in use for far too long and that the British hadn't bothered to change them. Knowing, however, that the moment war was declared the Royal Navy would almost certainly introduce both new codebooks and new enciphering tables, Tranow and his team worked as hard as they could from 1937 to 1939 to decrypt the British naval codes, while their system of codebooks and enciphering tables remained unchanged.

The Germans Take Advantage of British Coding Mistakes

To attempt to decrypt the British naval ciphers, Wilhelm Tranow and the B-Dienst obviously needed raw material from which they could work. They were dependent on the existing network of German radio monitoring stations to provide them with intercepted messages from British naval radio traffic. The stations at Lauf, in Bavaria, on the cattle ranch outside Seville, in the Canary Islands and on the Spanish coast provided these. B-Dienst also asked them to monitor British naval exercises off Sierra Leone in the eastern Atlantic in 1937 and any deployments in the Mediterranean, and used these intercepts as raw material that helped them begin to break into the British codes. How did they begin to do this? Firstly, the German monitors were alerted to listen out for the specific indicators at the beginning of the messages sent by the Royal Navy's ships, which alerted the intended recipient on another British ship, or at the Admiralty in London, that a message had been sent.

In an imagined scenario, the Royal Navy cruiser HMS *Hereford* is in the western Atlantic, on exercise with a mixed flotilla of one other cruiser, destroyers, frigates and fleet auxiliary ships, and they are practising refuelling at sea. It is 1937, and the flotilla is operating out of Freetown, the capital of Sierra Leone. The city had been an operating base for the Royal Navy since 1808, when it was the headquarters of the Royal Navy's West Africa Squadron, there to enforce the ban on the slave trade. When Royal Navy ships intercepted a slaver, and freed its captives, they brought them back to Sierra Leone, and liberty, hence the capital's name. Now, in the late 1930s, the port was a staging post not just for British naval and merchant ships

transiting from the South Atlantic, or from the Cape of Good Hope, but for Royal Navy vessels on exercise.

HMS *Hereford* sends a message to British naval headquarters in Freetown, saying '*Exercise completed, flotilla returning to port 1800hrs.*'

As the message is one of a very routine nature, it is not copied to the Admiralty in London. Naval headquarters in Freetown will almost certainly provide London with the details of the flotilla's exercises in a longer updating message. So as the message is only going from ship to shore in Freetown, the duty radio technician on HMS *Hereford* asks the signals officer whether the message is important enough to be sent encoded or simply in clear. If it doesn't need to be encrypted, then he takes the four- or five-figure groups direct from the codebook, doesn't encipher them, and simply sends them in Morse code. If the message is to be encoded, then the radioman goes to his copy of the Naval Cypher and finds the requisite four- or five-figure groups that correspond to the words 'exercise', 'completed', 'flotilla', 'returning', 'port' and '1800'. He then enciphers these using his subtractor tables, adds on the requisite indicators as suffixes or prefixes, or in the body of the message, as per the weekly or monthly or daily protocol specified to him by the ship's radio officer, and sends the message in Morse code. In the case of an enciphered message, the four-figure unenciphered destination indicator for Royal Navy headquarters in Freetown is, say, 9308; enciphered it's 5177. This is put at the beginning of that day's message, so the German radio monitors in the Canary Islands or outside Seville are listening out for messages beginning with either of these four-figure groups. When they hear them, they immediately listen to the entirety of the message that follows. The resultant four- or five-figure groups are written in one precise, sequential message on a typewriter, which is then sent by teleprinter to the B-Dienst at Flensburg-Mürwik or in Berlin, marked for the attention of the section that deals with the messages of the Royal Navy. In practice, the message will arrive in front of Wilhelm Tranow. The cryptanalyst and his team then look at the message to see if it contains any figure-groups that have been seen in other British naval messages. If so, these act as further confirmation that, for instance, 6533 transmitted in clear in Morse code is the Naval Cypher figure group for 'battleship'. The typewritten series of number groups are laid out above any other messages the Germans have also intercepted sent to or from naval headquarters in Sierra Leone. The German cryptanalysts then compare these to see if there are any recurrent groups. If there are, and the message is

decipherable, then it is the turn of the translators. Tranow or one of his deputies will then decide if the message in question merits onward transmission to Kriegsmarine Headquarters, or if it simply serves as further raw material for their ongoing cryptanalytical efforts.

•••

Wilhelm Tranow then discovered that although the British surface ships, submarines and small gunboats might be using different codebooks, they were using the same enciphering tables for all of them. Regardless of how complex the Naval Cypher No. 1, or its cryptological brother the Naval Code, might be to read into, this became immaterial if the Germans could read backwards into the codes from their encipherment tables. This meant that in order to be able crack three different codes used by the Royal Navy, the Germans only had to crack one set of subtractor tables. It was similar to having one set of keys that fitted three complex locks. This was a huge step forward for them. The British, helpfully for Tranow and his team, also had a habit of sending non-confidential messages in the Administrative and Auxiliary codes in 'clear', without enciphering them. So for instance, if the word 'destroyer' in the Administrative Code book was represented by the four-figure group 8344, then the British signalman would just send 8344 in Morse code. This code was originally invented to send the letters of the alphabet represented as a series of one, two, three or four dots and dashes, with the sound duration of the dash three times longer than the dot. Numbers from one to nine, however, were represented by groups of five dots or dashes. Thus 1 became dot-dash-dash-dash-dash, 2 was dot-dot-dash-dash-dash, 6 was dash-dot-dot-dot-dot, and 7 was dash-dash-dot-dot-dot. This made it simpler for the Germans: they applied the same principles for solving substitution codes to these British Morse transmissions. Say, for instance, that from comparing different messages sent in one of the three codes, the Germans suspected the words for port, starboard, signal, cruiser and submarine were represented respectively in the deciphering tables by the numbers 2665, 8120, 6887, 2017 and 5348. If one of these numbers was sent in Morse, in clear, in a message that made sense, then they had the correct number, and could add that number as the representative code encipherment for these four words.

Although the Germans were obviously interested in keeping their

cryptanalytical advances secret, they were astute enough to know that if some of their Allies – Italy, for instance – were engaged on the same work, then it made sense at least to offer to share some of their findings. Even by the start of the war, the Italians too had started making inroads into Royal Naval codes. Admiral Luigi Donini was one of the senior cryptanalysts in the Italian navy from the late 1930s onwards, and although the extent to which he passed cryptanalytical information to the Germans is unclear, he was certainly trying to break into the same British naval codes as Wilhelm Tranow, so his observations are very valid. He claimed that some of the main British mistakes were as follows:[1]

i. The British re-used the same key sequence over and over, leading to 'depths'.
ii. The period of validity of the enciphering tables was not commensurate with the level of radio traffic.
iii. Numerical sequences from an old table were sometimes added into the new ones.
iv. For many years the indicators were not enciphered, thus making it very easy to locate 'depths'.
v. When enciphered indicators were first used the method was so clumsy that it caused the Italians only a two-week blockage.
vi. The British Royal Navy cipher book did not contain homophones, in as much as it did not assign two or more code groups for two words that were differently spelled but pronounced the same – for example, 'allowed' and 'aloud'. Signals also began in true British style, with a complete address of 'to' and 'from'.
vii. Often most revealingly, 'geographical names were coupled, as an alternate interpretation, to vocabulary entries beginning with the same two or three letters. e.g.: 7184 = Give/Gibraltar, 0921 = Last/La Spezia, 4650 = Make/Malta, 2935 = All Concerned/Alexandria, 7714 = Left/Leghorn. This was of great help in identifying the geographical term when we had already identified the vocabulary term coupled thereto and vice versa.'
viii. The biggest mistake was the failure to introduce new code and cipher books at the start of the war: 'In my opinion, however, the most serious British carelessness or inadvertence was to keep in use for the whole first year of war with Germany the same principal Naval Cypher which was

in force since the time of the Spanish Civil War, broken by us (and by the Germans) in 1938.'

In summary, the main codes and ciphers used by the British Royal Navy around the start of the war were as follows:

Naval Cypher No. 1: A four-digit code group book, in force since 1934, for use by naval units. Naval Cypher was always used reciphered or doubly enciphered, a process known as super-encipherment. Reciphering or super-encipherment consisted of adding to the cipher a random-seeming number from tables of 5,000 number groups, but which, depending on the cipher, could be as many as 20,000 number groups. Naval Cypher super-encipherment tables at that time were limited to five; Commander-in-Chiefs Table, Flag Officers Table, the General Table held by all ships below destroyers, Small Ships Table and China Gunboats Table.

Naval Code, also known as the Administrative Code: A five-digit code group book, also in force since 1934, for communications to merchant shipping. It had deliberately been given a name that sounded similar to the Naval Cypher. For non-confidential signals it was used uncoded, and only from 1938, to the benefit of Tranow and his colleagues, recoded using one general series of tables, for confidential signals.

Auxiliary Code No. 3: A four-digit code group book, in force since February 1937, for use by small vessels such as Motor Torpedo Boats. It had been used unrecoded for non-confidential traffic and recoded by a multiple-alphabet table for confidential traffic. These two codes above were to be withdrawn from use on 20 August 1940.

By August 1939, despite his staff shortages, Wilhelm Tranow estimated that he and his men were reading the British Administrative Code, Auxiliary Code and the Naval Cypher No.1 about 35–40 per cent of the time. And this was at the height of his lack of personnel. Fortunately for him, his department was about to double, then triple in size.

The Organization and Running of the B-Dienst

During the first four years of World War II, the headquarters of the B-Dienst was located in the Tiergarten district of Berlin, overlooking the Landwehr Canal. The organization's offices were in the five-storey buildings at numbers 72–76 Tirpitzufer. Some of them were in the east wing on Bendlerstrasse,

which led to it being named the 'Bendlerblock', and in such a central, Teutonic and imposing location, there was an equivalently imposing head of the organization. Hermann Leopold Ludwig Eugen Hans Heinz Bonatz was a career German officer who was forty in 1939. He had joined the German Imperial Army in 1914, and then after the war transferred to the navy. As a senior lieutenant he commanded a torpedo boat. By 1937 he was a lieutenant commander, rising to be a captain and a staff officer in August 1939. He was on the vice admiral's staff for naval operations in western Europe, and had been serving with the B-Dienst part-time and unofficially since 1934. By 1939 his full title there was Chief of German Naval Radio Intelligence, the head of Group III (Radio Intelligence, Interception, Traffic Analysis, Cryptanalysis) of the B-Dienst of the Oberkommando der Marine. His subordinates, including Tranow, just called him 'Captain'.

Wilhelm Tranow was not just the senior cryptologist at the B-Dienst, and the head of the English language codebreakers, he was its senior civilian, with the rank of *Oberregierungsrat.* This was a post of a senior civil service councillor, and he was also in charge of the English 'desk' of Section IIIF, of 4/SKL of the OKM. Section III of 4/SKL stood for the third group of the fourth section of the *Seekriegsleitung,* which meant the Maritime Warfare Command. He was thus responsible 'for the interception of enemy radio communications, the evaluation of those enemy crypts, and the deciphering of enemy crypts'. He was also in charge of radio security and cryptanalytical security. Underneath him was a structure that, like that of OKW-Chi, was organized with characteristic German efficiency.

In Section I, there were four sub-sections, mainly dealing with training, administration, personnel and setting up of line telegraphy units. Section II's departments dealt with liaison with other units, operational secrecy, radio signal camouflage, deception and radio jamming, as well as managing the all-important teleprinter service which passed signals to and from the outlying intercept stations. It also handled the evaluation of captured documents, the allocation of radio frequencies, and the production and development of all cipher material, keys, systems and operational aids. In addition, Section II's sub-units monitored its own cryptographic material in a manner designed to simulate enemy decryption processes, while also developing its own new cryptographic material. Section II also developed IFF (Identification Friend or Foe) recognition systems to ensure that German naval units could recognize each other at sea, and lastly, they updated and published the crucial

Signal Book, or *Signalbuch*, of the navy.

The B-Dienst's meteorological department worked on all operational aspects and problems of transmission in the meteorological service, including the distribution of instruments, preparation of weather transmitters, allocation of frequencies for weather circuits, management of encryption of weather reports and unit management for line telegraphy of the weather service. For the German weather ships which were employed out on the maritime frontiers of the war, from around Iceland to the Azores to the western Atlantic, Section II was their technical quartermaster.

Section III was the cryptanalytical centre, the Communications Intelligence Department. It tracked enemy shipping, especially convoys; evaluated British, Russian, French, Swedish, Turkish and American signals intelligence, and processed, monitored and decrypted, then analysed, these signals. The most important of these for the B-Dienst was British signals, and first and foremost among these were those of His Majesty's Royal Navy.

PART TWO

GERMANY OFFENSIVE

Chapter Six

TWO NAVIES AT THE OUTBREAK OF WAR

At the outbreak of war, the administration of the German cryptographic systems was individually highly organized, but in collective disarray. In all, as listed before, there were ten separate and different agencies, units or offices whose responsibilities included cryptanalysis and signals intelligence. Out of these, there were six main ones: the army, navy, air force, foreign office, army headquarters and Göring's Research Bureau. Each of them had a separate agenda, and was answerable to different branches of the armed forces, the Foreign Ministry and the central security structure of the National Socialist Party. Wilhelm Fenner and the OKW-Chi had set up a focal network of monitoring stations and were concentrating on intercepting signals sent by some ten different nations, including the French, British, Russians, Italians and Turks. Their central role was still one of interception and linguistic interpretation, and by the outbreak of war, as the department expanded to between fifty and eighty personnel, it was ability with languages, rather than cryptography, that Fenner was looking for. The brilliant mathematician and astronomer Erich Hüttenhain and his trusted assistant, Walter Fricke, were in a minority as they devised encryption systems for the German army, the Heer. At the Foreign Office, Pers-Z were already reading the diplomatic codes of neutral countries like Ireland, Portugal and Norway, and had begun breaking into Swiss Enigma traffic.* But there were only eighteen people in

the agency's Berlin headquarters. Kurt Selchow, the head of department, was already falsifying some of the information gleaned from the signals his staff worked on. This was in turn passed on to Göring's headquarters. The covert resistance to the SS, the Reich Security Main Office and Hitler had already begun. OKL Chi-Stelle, the Luftwaffe's signals agency, was hard at work disseminating information that exaggerated its tactical abilities; as the Third Reich then possessed the most technically advanced air force in the world, it took little to persuade the French, the Poles and the Russians that the pilots and aircraft who had bombed Guernica in Spain were almost undefeatable. In preparation for the Wehrmacht's assault into western Europe, the regular army's cryptographers and signals monitors were preparing a full-scale deception plan to strategically outwit the entire French army and air force. Yet in terms of pure cryptanalysis and cryptology, Wilhelm Tranow and his naval staff at the B-Dienst were the most advanced.

The period from September 1939 to March 1940 gave the German navy's signals intelligence apparatus ample time to hone their skills, as the war fought in that period was almost entirely a naval one. Britain and France had signed military assistance treaties with Poland, and so two days after the invasion of that country on 1 September 1939, both countries declared war on Germany. However, the leaders of neither Britain nor France were in a hurry to attack Germany on its western border; both were very apprehensive of getting bogged down in another stalemate of trench warfare. As a result no major engagements took place for several months, and this period was called the 'Phoney War', or 'Twilight War'. When war was declared against Germany, Prime Minister Neville Chamberlain had appointed Winston Churchill to the position of First Sea Lord; Churchill wanted to begin more aggressive operations against Germany, unlike the pacific prime minister. Churchill ordered the Royal Navy to make every effort to find and engage the German warships that had left their home ports once war was officially declared. These included the battleships *Scharnhorst* and *Gneisenau*, and the heavy cruisers *Graf Spee*, *Admiral Scheer*, *Admiral Hipper* and *Prinz Eugen*. These large capital ships were more lightly armed but faster than any of the Royal Navy's battleships, and Churchill knew that if they broke out into the Atlantic shipping lanes, Allied supply convoys could be sunk indiscriminately. But also, he wanted the war fought, fought immediately, and if possible fought by his beloved Royal Navy.

•••

At 8.17am on 16 September 1939, thirteen days after Britain's declaration of war, two German radio monitoring stations picked up the same emergency signal from the same ship. OKW-Chi's most westerly listening station in Europe was at Lauf, and B-Dienst's was on the northern German coast. Both heard the same Morse code transmission, broadcast at 600 metres on the International Maritime Network: '*SSS … SSS … 49 N 38 W … Aviemore torpedoed … SSS … SSS … 49 N 38 W… Aviemore torpedoed …*'

'SSS' was the code used by the British Merchant Navy to signify that a ship was under attack by a submarine. The 4,060-ton British merchant steamer, with a crew of forty-four and a cargo of tin and iron plates, was en route from Swansea to Buenos Aires. On the morning of the 16th, the ship was 220 miles west of Cape Clear, heading into a dark Atlantic swell off the far south-westerly tip of Ireland. It was sailing independently and as dawn broke had crossed at right angles ahead of a British convoy, codenamed OB-4, westward bound to Newfoundland. The B-Dienst's listeners had picked up the signals of the convoy the night before, transmitted in the worldwide convoy code known as the International Code of Signals. They'd read them swiftly, and passed on the convoy's location to their headquarters at Neumünster by Enigma message; within minutes they were en route to the Befehlshaber der Unterseeboote, or U-boat headquarters, in Kiel.

Excited by this first convoy sighting of the war, Admiral Dönitz ordered the nearest German submarines to engage. U-35 and U-31 closed on the convoy at sunset, and followed it all night, and at dawn sent an Enigma-coded contact report with its heading, speed and number of ships. U-boat headquarters ordered every submarine in the English Channel and eastern Atlantic to attack. At 8.10am, Kapitänleutnant Johannes Habekost of U-31 fired two torpedoes at SS *Aviemore*, mistaking it for one of the ships in the convoy. The acoustic signalling and homing mechanism on one of his two *aale*, or 'eels', malfunctioned so only one hit, blowing a hole amidships in *Aviemore*, below the waterline. In ninety seconds the ship broke in two. In three minutes it sank.

The following day Wilhelm Tranow saw that in the harsh light of wartime, the signals interception and decryption network he had worked so hard to establish had functioned smoothly, and brought results. Listening in to the weather, position and emergency messages sent by Allied ships gave regular

cribs that enabled his cryptanalysts to reconstruct British parts of the merchant and naval codes. The speed with which the radio monitoring network could pick up a message and pass it on to the B-Dienst was measured in a matter of less than an hour if the listening stations knew exactly what they were looking for.

Within four weeks of the outbreak of fighting, Wilhelm Tranow and his fellow cryptanalysts at the B-Dienst had made considerable headway into reading and reconstructing the codes of the British Royal Navy, and its merchant auxiliary. Before the war, he and his men – his staff were still entirely male – had come up with another way to find cribs into the British naval codes. They had realized that merchant ships which had their home port of registration within the British Isles, and which were insured with Lloyds of London, sent this organization a radio message every day reporting their position. This information was then published in the gazette known as the Lloyds List, which was openly available in London. With assistance from OKW-Chi and its string of listening stations, they were already reading the Interdepartmental Cypher, used for communications between the Foreign Office, the Colonial, Dominions and India Offices, and the three armed services. But their crucial advance was continuing to read into the British code that was their key target: the Naval Cypher No. 1, used by all the ships in the Royal Navy to communicate with each other and with the Admiralty.

This was another encryption system based on four- and five-figure codebooks, with their encipherment carried out on subtractor tables. As soon as war broke out, the British changed this code, and introduced a new one which was simply called Naval Cypher No. 2. However, within six weeks Tranow's men had started to reconstruct this new one, as it was based on the same system of encipherment and decipherment as the old one. With a number of sub-variations, it was now used by the entire British Royal Navy, which at the outbreak of war was the largest in the world. It contained 1,400 ships, including seven aircraft carriers, fifteen battleships and battlecruisers, sixty cruisers, sixty submarines, 184 destroyers and numerous other vessels under construction.

But even though they had now changed the principle naval code, Tranow immediately noticed that there was a flaw that could help him and his colleagues break into the vital British cipher. The wily cryptanalyst noticed that the British submarine service were still using a variation of the old code, Naval Cypher No. 1. They had an unexpected and individual system of

encipherment as well: each submarine would encipher its messages using a simple monoalphabetic substitution system called the General Recyphering Table. This was just one of a number of British naval encoding tables available to ships, submarines and the Admiralty, and the submarine service still used it. Well aware that a monoalphabetic substitution system could be quite straightforward to crack, the submarine captains and signals officers further encrypted it with the subtractor tables of the old naval cipher which had been in use since 1934. So whereas the British navy's surface ships began using the new Naval Cypher No. 2 as soon as war broke out, the navy's submarines didn't. They sent position reports each day which the B-Dienst's monitoring stations picked up, so Tranow and his colleagues could start reconstructing the new Naval Cypher No. 2 by using this as a 'crib', or a word or group of words that could provide a way of breaking into the code. For instance, a British submarine or ship would provide a 'crib' by sending a coded message whose details the Germans already knew because it contained the same information as a message sent by one of their own ships. If a German cruiser was at a certain longitude and latitude at a certain time on a certain day, and a British vessel sent a coded sighting report of her, it stood to reason that much of their coded message would contain details – position, date – that the Germans already knew. The ability to use the position and contact reports sent out by Allied ships as 'cribs' was to stand the B-Dienst in good stead in the Battle of the Atlantic, the opening salvo of which was the sinking of the *Aviemore*.

•••

HMS *Rawalpindi* was a British P&O ocean liner of nearly 17,000 tons. It was named after the garrison town in India, and from 1925 had carried 600 passengers on each return voyage on the London to Bombay run. At the end of August 1939 the Admiralty informed P&O that they were requisitioning the ship, and converting it into an armed merchant cruiser, which would protect convoys. It took less than six weeks for the welders at Harland and Wolff's huge shipyards in Liverpool to attach eight old six-inch guns, and two three-inch, to the liner's decks. Its third active service patrol began in October, as it headed into the North Atlantic towards Iceland. On the 19th, it intercepted a German tanker which had been trapped in Buenos Aires when war broke out, and was racing to get home to Germany. As the

Rawalpindi watched the German crew scuttling their ship, its wireless operators repeated the same position report sent minutes earlier by the crew of the German tanker. The tanker's message had been sent on an Enigma machine, in a code called 'Tibet' reserved for the ships of the German Merchant Navy who found themselves trapped in foreign ports when war broke out.

One of the B-Dienst's monitoring stations on the Baltic picked up both signals. Tranow and his men had already constructed the British Merchant Ships Code, and could see that *Rawalpindi* had sent its position report using this encipherment. The Kriegsmarine's headquarters then informed all German ships in the area that an armed British cruiser was operating near Iceland. 23 November found *Rawalpindi* patrolling north of the Faroe Islands, in a freezing sea circling down from the Arctic Circle. The gun crews on its forward decks were standing four-hour watches in the almost horizontal sleet as the ship pushed forward over the waves. At such times in such conditions, the low temperatures often meant that the hoods and fronts of the men's duffle coats could freeze as they stood facing into the wind, and the service-issue towels that the sailors wrapped around their necks to stop seawater dripping down their collars also froze solid. Royston Alfred Leadbetter was a pre-war steward with P&O, who transferred to the *Rawalpindi* a few days after war broke out. His brother served on the same ship, both of them manning different three-inch gun positions.

> Half way into our third patrol at 3 pm on November 23rd 1939, the alarm bells sounded and I made my way to the boat deck. It was almost dark and it was freezing cold. In the poor light it was possible to see two grey shapes approximately five miles away. Suddenly a spout of water rose up a few yards away. It was quiet and at first we thought it was one of our own ships mistaking us for the enemy. Captain Kennedy and a midshipman came by and we were informed that there was a German ship near by, and that we were going to lay a smoke screen. Thick black smoke came from the funnel, but the smoke floats failed to work as it was too cold! After a short while the German ships opened fire.[1]

The lookout high in *Rawalpindi*'s forward crow's nest had spotted top masts and superstructure moving up and down on the horizon. The British navy needed as many men as they could get their hands on at that time, so

Rawalpindi's commanding officer was a sixty-year-old Royal Navy captain brought out of retirement. Edward Coverley Kennedy was certainly not lacking in courage. Looking through his binoculars, he thought the ship on the horizon was the German battleship *Deutschland*, so he sent a radio message to the Home Fleet reporting its position, and then steered for the cover of a fog bank, and a large iceberg four miles away. Coverley Kennedy ordered the ship's gun crews to close up, put the vessel at action stations and sent out a signal that said simply '*Enemy vessels sighted. Am engaging*.' Unfortunately for him and the crew of the HMS *Rawalpindi*, there were two German ships in front of him, the battleships *Scharnhorst* and *Gneisenau*, which were accompanied by two cruisers and five destroyers. Kennedy told his wireless room again to signal their position immediately, meaning that the B-Dienst also knew his exact position. Simultaneously the two German ships were radioing details of theirs. The *Gneisenau* flashed a Morse message to *Rawalpindi*, telling it to heave to, and stop wireless transmissions, or they would open fire. Coverley Kennedy refused, and at maximum range, gave his forward gun crews a one-word order. Shoot. They hit the *Scharnhorst* with their first shot; it then took thirteen minutes for the *Scharnhorst* to sink *Rawalpindi*: it went down with 238 men, including its suicidally brave captain, leaving thirty-seven to be picked up by the Germans. Royston Leadbetter's brother was killed on board the *Rawalpindi*, but he himself made it into a lifeboat:

> We gradually drifted away and watched as the *Rawalpindi* blew up and finally sank. One of the German ships saw us and stopped while we drifted towards it. The remarks shouted down to us, in English, were about the cold, hot tea, and their 'ancestry' from us. Suddenly the Germans called down and said, 'Sorry we cannot stop, one of your ships is near. Good night and good luck.' They then went off, nearly drowning us in their wash.[2]

Another British converted liner, the HMS *Chitral*, wisely waited before the Germans had sailed out of sight before rescuing another eleven men who, despite the almost sub-zero sea temperatures, were miraculously still alive. One of them was Leadbetter:

> A week later we landed in Glasgow, from there we were sent to London

> for questioning and then sent home with a rail warrant and £5. My mother came home from chapel to find two telegrams on the mat. One to say she had lost a son, the other to say another son was among the survivors. She never said which telegram she opened first.[3]

The action, meanwhile, had proved to the B-Dienst that their signals interception and decryption worked well, under pressure, at speed, in wartime conditions.

•••

On 1 October the British Admiralty had transmitted a message to every British merchant ship in the world. A German 'commerce' raider was operating off the east coast of South America. The 10,000-ton British merchant ship SS *Doric Star* was in the Indian Ocean when it received the message from four separate radio stations, broadcast in the International Code of Signals, with a naval appendix. The first came from the naval base at Simonstown outside Cape Town. Then the *Doric Star* heard it relayed onwards from the Falkland Islands and from Freetown in Sierra Leone, and lastly from the Admiralty broadcasting station at Rugby in Warwickshire. The Admiralty thought that the ship was probably the *Panzerschriff*, or pocket battleship *Admiral Scheer*. Armed with six eleven-inch guns, the heavy cruiser was faster and better gunned than anything the Royal Navy had in the South Atlantic. By December, the German raider had sunk six cargo ships. Each time it would signal its target merchantman by lamp, take off the crew, and then sink the cargo vessel with gunfire. The prisoners were then transferred to the supply and oiling vessel *Altmark*, with which the German heavy cruiser was operating.

On 1 December, the *Doric Star* was sailing in warm waters and under skies that saw daily sun, some 660 miles south-east of St Helena in the South Atlantic. It was heading north-west towards the equator and Great Britain with a cargo of refrigerated lamb, beef, butter and cheese, along with bales of wool. The sea was calm. Suddenly a shell exploded 100 yards off its starboard bow, followed closely by a second. The only sign of a ship that the captain of the *Doric Star* could see was the top of a superstructure on the port horizon. He ordered the ship's wireless operator to broadcast the raider distress call, asked the engine room for full ahead, and pulled north. Instantly, he saw a

daylight Morse message flashing from the enemy ship, signalling him to stop his engines, and stop his wireless. He obeyed the first instruction, and ignored the second. He told his chief engineer to prepare to scuttle the ship, and as he did so, he saw the heavy cruiser *Admiral Graf Spee* steam into view, like a long, grey panther. He instructed the radio room to send the emergency three-letter 'BBB' message instantly, meaning he was under attack by a battleship. Another Morse message followed from the German: '*Stop your wireless or I open fire*.'

Seconds later a British ship, HMS *Ajax*, repeated back that it had heard *Doric Star*'s emergency message. The captain cancelled the order to scuttle, and gave orders to throw overboard the ship's codebooks, weapons and radio equipment. The *Graf Spee* sent a motorboat with a boarding party of three officers and thirty men, who searched the ship, ascertained that the *Doric Star* had broadcast a distress call, and examined the bales of wool in the hold. The German sailors missed the chilled holds full of meat, to the later chagrin of their Kriegsmarine colleagues, deprived of fresh rations after months at sea. The crew of the *Doric Star* were given ten minutes to collect lifebelts, blankets and personal possessions; the Germans looted the ship of sextants, chronometers and binoculars, and took off the crew. They made a particular effort to look for any radio codebooks or transmitting equipment. An hour later seven 5.9-inch shells and a torpedo from the *Graf Spee* sank the merchant ship.[4]

When the SS *Doric Star* had broadcast its two distress calls, five separate radio operators had picked them up. One was the British light cruiser HMS *Ajax*, steaming off Argentina, the second a Greek freighter, the third the duty wireless operator at Simonstown, the fourth was the *Altmark*, and the fifth the *Graf Spee*. The Kriegsmarine's B-Dienst had decided to broaden the base and worldwide range of their signals monitoring system by installing radio listening equipment in the wireless rooms of Germany's cruisers and its nine capital ships that had already been launched: *Bismarck*, *Graf Spee*, *Tirpitz*, *Admiral Hipper*, *Deutschland*, *Prinz Eugen*, *Admiral Scheer*, *Scharnhorst* and *Gneisenau*. (*Tirpitz* and *Bismarck* would not be fully operational until 1941.) The *Doric Star*'s two messages – the raider distress call and the repeated 'BBB' message – were broadcast in Morse, so neither the German battleship nor its supply vessel had need to decrypt them, nor forward the messages back to Kiel.

Radio Signals Deception by the *Graf Spee*

Helmut Ruge was twenty-two in winter 1939, a Kriegsmarine NCO from Cuxhaven in northern Germany who had trained as a radio operator. He had grown up during the economic depression in the 1920s, and then joined the navy. He joined the *Graf Spee* shortly before war broke out, when it sailed on 20 August 1939 for South America on a thinly disguised public relations voyage. By the time December came, and its tally of sunken merchantmen was rising, Ruge and his twenty-nine colleagues in the battlecruiser's signals section were already using British Merchant Ships codes in an elaborate game of electronic bluff. There were civilian decryption personnel on board the ship when he joined it, and as he spoke some French, he was given the job of helping them as they tried to break their way into French and British naval codes. By the time the ship arrived in the Indian Ocean and then the South Atlantic, they had captured some British Merchant Ships codebooks:

> We were able to crack one of the British radio codes when one of the merchant ships that we sank failed to destroy their code book. When we approached this particular ship, we instructed them not to transmit any messages or we would open fire on them. Despite our order, we heard the ship start to send a message and sent this information to the 'Graf Spee's' commander. The 'Spee' then fired a short burst from the 2cm machine guns at the merchant vessel's bridge, as a result of which the radio operator was wounded and was unable to destroy his code book, hiding it instead behind his transmitter. Once we boarded their ship we found the code book which we took back, together with their radio transmitter to the 'Spee'.
>
> With the code book and the enemy ship's radio transmitter we were able to send false messages which would make the British believe, for instance, that we were in the North Atlantic, not the South Atlantic and create as much confusion as possible. We always tried to communicate, with the enemy ships we sank, by signal lamp because to use radio contact would give our position away to the British. However, if one of these ships was able to get off a radio message before it was sunk, we had nothing to lose by using our radio and would then take the opportunity to send our own messages to Germany advising them of the ships we had sunk and the cargoes they were carrying.[†]

Hunting the *Graf Spee* was the Royal Navy's Force G Cruiser Squadron, searching the southern Atlantic for the German commerce raider. The two heavy cruisers HMS *Cumberland* and *Exeter*, with eight-inch guns, and the light cruisers *Ajax* and *Achilles*, armed with six-inch guns, were just one of eight task forces that the British Admiralty had ordered to search for the *Graf Spee*. Force G was commanded by Commodore Henry Harwood. They broadcast their signals in the Naval Cypher No. 1, which, as previously mentioned, Wilhelm Tranow and the B-Dienst had started to crack in 1934, finally succeeding in 1938. The efforts put into deciphering the signals from the long summer afternoons on the cattle ranch north of Seville, where the OKW-Chi had their southernmost Spanish station – tuning in to the loose-lipped British naval wireless operators communicating from battleship to cruiser to destroyer off Sierra Leone in 1937 – had been worth it. So the B-Dienst in Germany, and by extension the *Graf Spee*, almost certainly knew what the British warships were saying.

At 1.15pm on 3 December 1939 Harwood sent the following signal to the other ships of the Royal Navy's 'South American Division', which was the full operational name for the ships in his task force, the cruisers *Cumberland*, *Achilles* and *Exeter*.

> In view of report pocket battleship, amend previous dispositions. CUMBERLAND self-refit at Falkland Islands as previously arranged but keep at short notice on two shafts. ACHILLES leave Rio de Janeiro area so as to arrive and fuel Montevideo 0600 (Zone plus 2) 8th December, EXETER leave Falkland Islands, for Plate a.m. 9th December, covering S.S. LAFONIA with returning volunteers. AJAX, ACHILLES concentrate in position 35 degrees south, 50 degrees west at 1600 (Zone plus 2) 10th December. EXETER to pass through, position 090 degrees Medanos Light 150 miles at 0700 12th December. If concentration with AJAX and ACHILLES is not effected by that time further instructions will be issued to EXETER. Oiler OLYNTHUS is to remain at sea rendezvous until situation clears instead of proceeding to Falkland Islands.[5]

After sending this signal, strict radio silence was imposed, but it was enough. It was the signal that Wilhelm Tranow and the B-Dienst, in their headquarters at Tirpitzufer in Berlin, and even Ruge's colleagues on the *Graf*

Spee, would have been waiting for. Did they read the signal almost simultaneously, and direct the Kriegsmarine to signal directly back to *Graf Spee* that it was facing only three ships, and not four? If Captain Hans Langsdorff of *Graf Spee* had received this information, he now knew he had a fighting chance. The fact that he decided to do battle suggests that he did receive a signal, although neither the radio room on the *Graf Spee* nor B-Dienst records confirm this.

By 12 December, HMS *Exeter*, *Ajax* and *Achilles* were steaming off Uruguay, and the *Cumberland* was still refuelling and refitting at Port Stanley in the Falkland Islands. Harwood had written the British Royal Navy War College's textbook on how cruisers should attack a battleship, and when his task force sighted the *Graf Spee*, he knew instantly that he had to do three things. Attack at once, split the German ship's fire, and stop it retreating back to Germany. If he had had HMS *Cumberland* alongside him, he would have had parity of firepower with the pocket battleship, but until the heavy cruiser could make the 1,100-mile voyage north, there was just *Exeter* and the two light cruisers. The rules he had written himself dictated that if Harwood went into the attack during daylight, he would put *Exeter* with its heavier eight-inch guns with its back to the rising sun, and open fire as it came up. *Graf Spee*'s eleven-inch gun crews had a 4,000-metre range advantage over *Exeter*, so Harwood knew that he would have to sail close. *Ajax* and *Achilles* would steam the other side of the German ship, meaning that it would have to divide its two turrets either right and left or forward and aft. If he attacked at night, the British ships would attack in a line from one side.

Harwood also knew that to win the battle he had to achieve one of three things: sink the *Graf Spee*, force it to surrender or scuttle, or damage it sufficiently so that it would be unable to make the long journey home to Germany. To return home, it would still have to run the gauntlet of the British Home Fleet in the Channel or North Sea. If it was damaged in the South Atlantic and was limping home, it would stand an even chance of being sunk. The idiosyncratic tactical and strategic diktats of the comparative layout of forces thus meant that even if the *Cumberland* did not reach him in time, Harwood lost all three of his ships, and the *Graf Spee* was only damaged, he would still have won the strategic battle. The Germans had only eight capital ships, and three months in from the outbreak of war could not afford to lose one, whereas for the Royal Navy, three cruisers was an acceptable loss. So with this harsh reality in his mind, Harwood prepared to

do battle.

At 6.14am on the 13 December 1939, *Ajax* spotted smoke. Harwood ordered *Exeter* to investigate, and two minutes later its signals lamp announced, '*I think it is a pocket battleship.*' HMS *Exeter* ran the signals flag 'N' up to its yard arm, indicating '*enemy in sight*'. It signalled to the Admiralty that it had a battleship in sight, and was engaging. Langsdorff then attacked, accelerating towards the British ships at top speed, opening fire at 6.18am from nearly eleven miles away. On *Exeter*, the gunnery officer was Lieutenant Commander Richard Jennings. As he was crossing the compass platform to action stations, still in his pyjamas, the captain hailed him, not with the normal formal language of 'Enemy in sight, bearing etc.', but with 'There's the fucking *Scheer* !' Throughout the battle the crew of the *Exeter* thought they were fighting the *Admiral Scheer*. But the name of the enemy ship was of course the *Graf Spee*.[6]

The Battle of the River Plate turned into a slugging match. HMS *Exeter* took thirty-six hours of repeated hits, but the gunnery skills of its three turrets meant it was able to fire repeatedly at *Graf Spee* from seven miles away and score impacts, while sailing in a semi-circle at twenty miles per hour. Three things impeded Langsdorff. Firstly and most importantly, the German ship's fuel system was hit and one gun turret put out of action. Secondly, the gunnery skills of the British were very good, and their ships, although older than the German, could take an enormous amount of punishment and keep afloat. So could the British sailors. At one point, Lieutenant Commander Jennings on *Exeter* was standing on top of the ship's rear turret, the only one left in action. With one eardrum burst from standing close to repeated gunfire, and blood pouring out of the other ear, he was still spotting targets from the top of the turret, and shouting fire control orders down through an open hatch.

Throughout the battle, the three British ships were waiting desperately for the arrival of the *Cumberland*, racing northwards from the Falkland Islands. Commodore Harwood knew that he had to try to fool Hans Langsdorff into thinking its arrival was imminent. He knew that at maximum revolutions, *Cumberland* would take thirty-six hours to steam north from the Falklands to the estuary of the River Plate, off Montevideo. In the radio room on *Graf Spee*, meanwhile, Helmut Ruge had a narrow escape:

While I was on duty in the radio office during the battle, which lasted

> four hours, a shell from one of the enemy cruisers passed through the radio office and lodged on a bunk in the next cabin, incredibly, without exploding. By a lucky chance for me, the crew on the British cruiser had fired a training armour piercing but non-explosive shell by mistake. Had the shell had an explosive warhead, I would have certainly been killed. My life had been spared. My knowledge of what was happening during the battle was restricted as I was in the radio office, but I was kept partly informed by the man who was in the Radar office who could see what was happening.[7]

The German captain then made the one error that lost him the battle. He decided to head for the supposed safety of the neutral harbour of Montevideo, instead of breaking off the action and heading for the North Atlantic. His superior firepower would have allowed him to keep Harwood's ships at bay, and by the time HMS *Cumberland* arrived, *Graf Spee* would have been across the equator, and, crucially, backed up by four U-boats that Admiral Dönitz had ordered towards Montevideo. But he headed for the estuary of the River Plate. As he did so, he was still being engaged by HMS *Exeter,* which now had only one gun turret functioning. A lucky shot from one of *Exeter*'s last eight-inch guns penetrated two of *Graf Spee*'s decks and exploded beneath one of its funnels, crucially damaging its diesel fuel supply system. It now could not return to Germany nor make repairs at sea, and the only port available to it was Montevideo.

All the British had to do was to wait for Langsdorff to leave harbour. To prevent him doing so, while they waited for reinforcements, they cleverly manipulated the international maritime laws governing the movements of shipping in neutral harbours. These stated that any warship from a belligerent nation, such as Germany, had to wait for twenty-four hours after an unarmed merchant ship from any of its enemy's fleets – such as Britain or France – left the harbour. This was, obviously, to stop it chasing them and sinking them. So the British embassy in Montevideo arranged for the port authorities to stagger the departures of a number of British and French merchant ships lying at anchor. Three days later, on 17 December 1939, Langsdorff scuttled his ship. His reasoning, he wrote, was that he was running low on eleven-inch ammunition, reducing his ability to fight for more than twenty minutes, and the British were trying to hold him inside the neutral harbour while HMS *Cumberland* and the battlecruiser HMS *Renown* arrived. He was right.

The battle had been a triumph for the use of signals intelligence: from the sinking of the *Doric Star* to the scuttling of the *Graf Spee*, the B-Dienst had been monitoring, intercepting and decrypting two sets of signals, merchant and naval, simultaneously. It hadn't been a triumph for the Kriegsmarine, however. Captain Langsdorff shot himself in the head with his service Luger pistol on 19 December, fearing he had lost one of Germany's capital ships unnecessarily. Although it had been the lucky shot from *Exeter* that sealed his fate, Germany now had only seven battleships and battlecruisers, and the war had been underway for only four months. But if the Germans suffered from a numerical inferiority in terms of large warships, they certainly did not in terms of another type of vessel: submarines. Each equipped with its own Enigma machine, they considered themselves the height of technological development, and also of covert communications. The Battle of the River Plate had been a small, practice run for the B-Dienst and its codebreakers in comparison with another campaign already underway – the Battle of the Atlantic.

---

[*] The German and American operations to read Swiss messages encoded on the Swiss Enigma machines are covered in Chapter 16.

[†] Helmut Ruge wrote a lengthy first-hand account of his wartime experiences in 2008, the year before he died. After the scuttling of the *Graf Spee*, he was interned in Uruguay, escaped by walking across the Andes to Chile, and boarded a German ship for Japan and thence another, the MV *Odenwald*, bound for Germany. This was captured and boarded by the Americans in the Pacific. His account can be found at ww2pacific.com, or at uboatarchive.net.

Chapter Seven

ROMANIAN CODES AND ROMANIAN OIL

In the second half of the 1930s, the Romanian military attaché at the country's embassy in Paris used a cipher that had withstood repeated efforts by the Germans to read it. The signals that were sent by the Romanian embassy in France were encoded, and dispatched in cipher by telegram to their army headquarters in Bucharest, from where they would also be forwarded on to the foreign ministry. OKW-Chi's listening stations had begun picking up some of these messages in 1936, but had been consistently unable to break into the code. Then in February 1939 the Paris embassy surprised Wilhelm Fenner's listening stations by sending a much longer message than usual. The Germans then noticed that a message of almost identical length had also been received, inbound to Paris from Bucharest. This signal consisted of two long groups, made up of sections of five letters from their alphabet.

Part of the difficulty was that the Romanian alphabet contains 31 letters, with two extra variants of A, and one each of I, S and T. These differentiations are marked by the use of diacritics above and below the letters. So apart from the normal twenty-six letters of the Roman alphabet, there were also five variations of four of the most commonly used letters. The OKW-Chi listening station at Lauf had intercepted the messages to and from Paris, recognizing them by the identifying 'indicator' code at the start of the

text, which the transmitting operator at the Ministry of Defence in Bucharest would use to inform the receiving operator in Paris of the correct message key to use to decipher the signal. If the operator was using an enciphering machine, like an Enigma, this indicator told him how to set the rotors on whichever machine he might be using. If a codebook was being used to provide the daily key, the indicator would refer to a daily coding setting that only a person in possession of the respective codebook and enciphering table would know. Once the Lauf interceptors had picked up such messages, they were sent by teleprinter to OKW-Chi's headquarters in Berlin. Erich Hüttenhain and Walter Fricke received them straight away. Hüttenhain and the Chi operators could see that the two lengthy Romanian messages dispatched a month apart in February and March 1939 were identical, with the exception of ten numbers. Hüttenhain now saw his opportunity. His advantage was that he had access to 'depth', as the Romanians were both sending and receiving two or more messages with the same key. Although he only had access to the encoded cipher text, he was able to carry out what he called a '*Geheimtext-Geheimtext-Kompromiss*'. Translated, this means a cipher text-to-cipher text compromise. He recognized that it was a '*Zahlenwürmer*' – a 'number worm', a long chain of numbers and a five-digit code that had been overwritten with a substitution. Following the same principles for substitution texts as the British at Room 40 in London in World War I, and as Wilhelm Tranow at the B-Dienst, he started a process he called, in German, '*Streifenverfahren*'. Literally translated it means 'strip-decoding process'. Or, simply put, strip decodes. When a cryptanalyst has a coded message of five letters, say, ANTPK, they can surround it with other letters to make the code more complicated to break. So it could be possible to have VBQANTPKMME. Removing the first three and last three letters is thus called strip decoding. Bearing in mind, too, that if the message in Romanian is ANTPK, there are six different permutations of this letter chain alone as there are three different versions of A and two of T.

All the recorded Romanian messages were successfully 'stripped' of their overwriting and the code that had been used was then decrypted. As Hüttenhain did so he found the reason for the cipher text-to-cipher text compromise. The Romanian military attaché in France had suggested in the first message, the preceding month, that the Romanian National Philharmonic Orchestra could give a concert in Paris. After all, he said, the Hungarian national orchestra had given a concert in the French capital

recently; and, not wanting to be outdone by their neighbours and occasional enemies, he suggested that Romania could do the same. In his message the defence attaché in Paris was drawing attention to a particular issue – number 15 – of a specific magazine. In this the entire musical programme of the Hungarian orchestra from the preceding year was laid out. The second long message that the Germans intercepted, inbound from Romania to France, had the same 'plain text' verbatim, but with one crucial addition. It contained one important query, because the Romanian cipher clerk in Paris had made a simple mistake with one number: instead of sending the number '15', he sent the number '17'. So the message had confused the recipients in Bucharest. They couldn't find any details of a musical programme for the Hungarian national orchestra in issue number 17 of the magazine in question. Had Paris perhaps made a mistake? The answer was yes. Two mistakes. The first was that the list of musical pieces was contained in issue number 15, and the second mistake was to do not with culture, but with cryptography. The Romanian coder in Paris had repeated the entire message when Bucharest contacted him again, saying they couldn't find the programme. So instead of sending a coded message that said simply '15 not 17' he sent a long string of numbers, a Zahlenwürmer, that contained the entire original message. So Hüttenhain had two large lumps of identical plain text to compare. And thus he broke the Romanian military code, and from early 1939 onwards, the OKW-Chi could read at least some of the signals sent to and from the military attachés at Romania's overseas diplomatic missions.[1]

As war approached, these messages started increasingly to specify Romania's strategic, economic and geopolitical position vis-à-vis Germany, and also in regards to its neighbour, Hungary. Hüttenhain and his colleagues were ordered to keep their eyes and ears open for every single message sent by the Romanians. For the wild, rugged country, with its capital described as 'the Paris of eastern Europe', was vital to Germany and its war plans as it had one commodity that was more important than anything else. A very great deal of oil.

Why Germany Needed Romanian Oil

In 1938, Germany consumed forty-four million barrels of oil, and knew that when war came, this figure would rise dramatically. Mobile warfare would, simply put, be impossible if the country could not guarantee itself a reliable

supply of oil. Germany got its petroleum products from three different sources: from domestic fields, from imports of crude oil and refined petroleum from abroad in the United States, the Persian Gulf and Romania, and from synthesizing petroleum products from coal. The Third Reich's armoured and mobile divisions could not go to war on air, and knew that when they declared war in Europe, their ability to import oil would be vital. The British would close and control the Suez Canal, and the United States would almost certainly impose a fuel embargo on Germany. This meant that Romania was crucial.

By 1938, Germany imported 60 per cent of its annual oil supply from overseas, amounting to some twenty-seven million barrels: another four million were imported overland from Romania, another four came from domestic production, and a further nine were produced synthetically. By the end of that year Germany had fifteen million barrels stockpiled. Although the Germans counted on being able to seize about five million more from the stockpiles of Norway, Holland, Belgium and France, all earmarked for invasion in 1940, and had guaranteed imports of another four million in 1940 from the Soviet Union, a campaign across Europe and possibly Russia would require seven and a quarter million barrels monthly. With only 5.35 million available from its own domestic production and overland imports, there would thus be an enormous shortfall. The Third Reich's military planners knew that if they were going to even begin to be able to sustain mobile warfare in Europe, Russia and even North Africa, as well as submarine and naval operations, all in the face of an economic blockade, then they would obviously have to be able to guarantee their oil supplies. They could fight in North Africa, seize the Suez Canal, destroy the Royal Navy in the Indian Ocean and seize the Persian oil fields around Basra. They could invade Russia and send armoured and mobile divisions fighting towards the Caucasus, seizing Ukrainian wheat and coal en route, heading for the oil fields of Baku and Grozny, which produced 200 million barrels annually. But obviously, neither of these options could be firmly guaranteed.

The Germans' only solidly dependable external supply of petroleum products came from Romania, from the oil fields around the town of Ploiesti, thirty-five miles north of Bucharest, in the wheat fields and valleys of the Muntenia region. The world's first large oil refinery was built outside the town in 1855. In World War I, the British sent a mission to sabotage these production fields before the German advance managed to reach them. The

task was given to Lieutenant Colonel John Norton-Griffiths, an idiosyncratic engineer and construction designer who had fought in South Africa in the Second Anglo-Boer War, and helped introduce tunnelling onto the Western Front as a way of countering German mine-laying operations. He had formed a unit composed of sewage workers from Manchester who could dig under German lines and place explosives. In Ploiesti, the eccentric colonel dumped cement into some of the wells, set others on fire, dropped nails in storage tanks, and destroyed 800,000 tons of crude oil and dozens of refineries. He was knighted for his efforts, although a senior British diplomat noted that within six months of his sabotage operation, the refineries were back to full production.

The Germans knew that if they took advantage of Austria's underdeveloped oil industry, they could probably triple their domestic production, but Romania was the economic ace of spades they needed in their hand. They were aware that if the country gave or sold even 50 per cent of its annual production to Germany, they could count on a crucial thirteen million barrels each year. What Germany did not want was Romania forming any kind of allegiance with the British, holding back stockpiled oil that it could be selling to the Third Reich, trading the vital fuel with Hungary for territorial concessions over Transylvania, or blocking riverine access on the Danube or rail links from Ploiesti. So the Germans concentrated on cementing their economic ties to the country. They were helped in this by the fact that they had begun to read into some of Romania's codes, and so could monitor and read some of its diplomatic and military signals, and gauge the country's intentions. This made breaking Romania's different ciphers one of the highest priorities for the Reich's signals intelligence and cryptographic apparatus in 1938 and 1939. To formalize relations between the two countries, both parties signed the German-Romanian Treaty for the Development of Economic Relations on 23 March 1939 in Bucharest. This was a bilateral economic treaty which established a very convenient and useful German control over most aspects of the Romanian economy, and it had the subsequent side effect of forcing the Romanian government to join in an allegiance with Germany and Italy. The treaty effectively turned Romania into a German dependency, said *Time* magazine in the United States, adding that 'in no instance of modern times has one state made such humiliating, far-reaching economic concessions to another'.[2]

The agreement was scheduled to become effective ten months hence, on 20

January 1940, and was registered as a League of Nations Treaty; its main provisions were that Romania should give timber, agricultural products and, most crucially, oil to Germany in exchange for military equipment and training, while German companies operating in Romania would benefit from access to free trade areas. The British were understandably alarmed by the signature of this treaty, and so offered to try to provide security guarantees to the government in Bucharest. On 13 April 1939, France and Great Britain decided that they should guarantee the independence of the kingdom of Romania, after similar discussions between Romania and the Soviet Union had collapsed when Bucharest refused to let the Red Army cross its borders.

But on 1 September, Hitler invaded Poland. Warsaw was expecting military assistance from Great Britain and France, and wanted to be able to evacuate its army, its gold reserves and as many civilians as possible into Romania; but although the country remained neutral, pressure from the Soviet Union and Germany saw it intern the fleeing Polish government after it had crossed the border into Romania on 17 September. With World War II now only days old, Romania, under King Carol II, decided to officially adopt this position of neutrality, but it swiftly proved impracticable as inside the country violent, popular Fascist groups such as the Iron Guard urged the government to form an alliance with Germany and Italy.

Although Britain and France had been the main guarantors of Romanian territorial integrity before the war, offering to back the country militarily in the event of outside invasion, in the actual event the alliance of the Iron Guard and the Axis powers proved much stronger. Into the bargain, Romania was hoping that Germany would be able to help it to keep its borders safe from Russia and Hungary but, unknown to the Bucharest government, the Germans had already decided to allow the Soviet Union territorial concessions onto Romanian soil under the terms of the 1939 Molotov–Ribbentrop Pact. Germany was aware that if Romania saw itself threatened by Moscow, it would be much more likely to devote the resources of its huge army and vital supplies of oil to Germany.

However, before such concessions could take place, the Romanian fascists and the army staged a *coup d'état* that put Marshal Ion Antonescu in power, and on 21 September 1939, Romanian Prime Minister Armand Calinescu was assassinated. The remaining government saw that, with war now underway, any alliance with Britain and France was going to be much less effective than an agreement with Germany, however one-sided it might be, so

they decided to cooperate with Berlin. In the event, it was to take Romania until 23 November 1940 officially to join the Axis alliance, although in practical terms it had done this long before. The new military regime in Bucharest, obligingly, did not change their military or diplomatic codes, so both in terms of oil, and codebreaking, the Germans were again triumphant.

In the middle of this complex political and economic bargaining, the Romanians had missed apprehending three very significant people who, unbeknown to them, had crossed their border from Poland after Germany had invaded it. Polish cryptographer Marian Rejewski and several others from the cipher bureau in Warsaw were evacuated to Romania before the German troops reached the Polish capital. After crossing the border, Rejewski and two others just avoided being forced into a refugee camp, and so made their way to Bucharest where they made contact with firstly the British and then the French embassy, who in turn helped them escape to Paris by train. By the end of September, with their native country in flames, these three key Polish codebreakers reached the French capital and joined a joint French, Polish and Spanish decryption unit based at the Château de Vignolles outside Paris. Two months later they were helping decode German messages encrypted on their Enigma machines: the Germans, meanwhile, still did not realize its secrets were compromised.

Chapter Eight

SIGNALS AND DECEPTION IN THE INVASION OF EUROPE

When war broke out, inter-agency rivalries among Germany's cryptanalysts were temporarily forgotten in the common cause of the invasion of Europe. With thousands of messages to intercept and decrypt, the staff of the army, navy, air force and Foreign Office signals intelligence agencies were swamped. On 1 September Germany had invaded Poland without a formal declaration of war; Norway, Switzerland and Ireland had declared their neutrality, although Switzerland mobilized its army. On the 3rd, Britain declared war on Nazi Germany after a deadline expired for the latter to withdraw its troops from Poland. France, Australia, India and New Zealand followed suit within hours, and shortly after midday on the 3rd, the SS *Athenia* was torpedoed west of Ireland. The United States and Japan declared their neutrality in the European war, and South Africa deposed its prime minister in favour of his deputy, Jan Smuts, with the country declaring war on Germany shortly afterwards. After announcing a naval blockade of Germany, Britain attacked the German battleship *Schleswig-Holstein* at anchor outside the Kiel Canal, but all of the RAF bombs that hit it failed to explode; Warsaw was surrounded by German troops, and by 19 September Russian and German forces linked up at Brest-Litovsk. On 28 September, the German–Soviet Boundary and Friendship Treaty was signed by foreign ministers Molotov and Ribbentrop, and the secret agreement specified the details of the way in

which Poland would be divided up, which had been first laid out in the original Molotov– Ribbentrop Pact signed on 23 August. On 28 September, the Polish army in Warsaw surrendered to the Germans.

Against this backdrop of a new war, the B-Dienst's partial cracking of the Royal Navy's codes meant that on 11 September 1939, the Germans could find, and then attack, a British merchant convoy even as it was forming up. In Spain, General Franco was still hesitant about joining the war, so Hitler sent Wilhelm Canaris to encourage him; some of Franco's and all of Canaris' signals were being read both by the Foreign Office and by Göring's codebreakers, as Hitler was already paranoid by this very early stage of the war about a plan to assassinate him and replace him at the head of the Third Reich with a moderate German, a leader who would sue for peace with Britain. By the end of 1939, Great Britain and France were the prime adversaries of Nazi Germany, and were their priority military targets. Japan and America still remained out of the war.

By late 1939, Wilhelm Tranow and the B-Dienst were succeeding in breaking into the Royal Navy's Naval Cypher No. 2, but only when it was enciphered with the same tables that were used by the British submarine service. The B-Dienst were now also able to decode some of the British Admiralty's weekly intelligence summaries sent to naval attachés at their embassies abroad, as this was sent in yet another of the variety of codes the Royal Navy and the Admiralty used – the Interdepartmental Cypher. Tranow and his team were also still reading British naval messages sent from the area in the Atlantic off Freetown, the capital of Sierra Leone; this was now a stopping point for convoys and their escorts as they sailed south to Cape Town or west to the Caribbean. Decoded, these provided intelligence on the movement of these new convoys and the destroyers and frigates that comprised their escorts. The British Admiralty also exchanged signals with diplomats in countries like Sierra Leone who gave them information about the movements of ships and convoys from neutral countries criss-crossing the Atlantic. When it came to reading the diplomatic and air force traffic of their enemies, the codebreakers from the OKL Chi-Stelle were also, by now, reading the communications of air attachés based in countries in the Near East, Portugal, Sweden and Switzerland. The maximum daily number of signals that comprised this traffic was about 100 messages, according to a later statement by Ferdinand Voegele, the Luftwaffe's chief cryptanalyst.[1]

Germany, its Cryptanalysts and the Norwegian campaign

After the outbreak of war in 1939, Norway made the decision to remain neutral, and mobilized its army, navy and air force to protect this status. It chartered 150 merchant ships to the British, as both parties saw that their maritime supply lines would be threatened by the Germans. Both countries knew they would depend on convoys to supply them, by crossing either the Atlantic or just the North Sea. Norway was important because of its ports and strategic shoreline, and because it produced large quantities of iron ore, and Germany needed huge amounts of this mineral for its armaments industry. The country also protected its northern flank, and during the winter, when the Baltic Sea was largely frozen over, access to Norwegian ports allowed German naval traffic to operate in the North Sea, while German aircraft could operate from Norway over the North Sea, the Atlantic and the crucial Denmark Straits between Iceland and the Faroe Islands. Norway aligned itself with Great Britain and Sweden in support of Finland when Russia attacked the latter at the end of November 1939. But by early 1940, the country could only field 9,500 troops to defend itself against a possible Soviet attack.

The British wanted Norwegian iron ore too. They thought if they sent units of troops to occupy parts of Norway and Sweden, ostensibly to help Finland, they could guarantee themselves access to Norway's minerals. The French, meanwhile, were very pleased by this plan, as it meant that the Germans would have other military commitments in Europe that might prevent them from striking westwards. Simultaneously, the German U-boat service were embarking on attacks on Allied shipping in the Atlantic, helped enormously by being able to read the British Merchant Navy's codes. The B-Dienst's success with decoding of British messages crucially revealed plans for an Anglo-French expedition against Norway, under the cover name of Operation *Stratford,* so Germany seized the initiative and invaded Norway on 9 April 1940. The naval codebreakers' fortunes then improved further: when Norway surrendered in early May 1940, the B-Dienst received a number of captured documents from HMS *Hardy*, a British destroyer which had run aground in the Ofotfjord in the Battle of Narvik. The British then went even further in their laxness with important documentation: when evacuating Bergen, they left behind a large cache of cryptography documents which were only discovered in May 1940. These included a copy of their Administrative Code, a copy of the Foreign Office Interdepartmental Cypher No. 1, the

current Merchant Ships Code with recoding tables, and the Auxiliary Code and recoding tables along with call-signs and delivery groups. For Tranow and the men at B-Dienst, this was Christmas and Easter and all their birthdays rolled into one. And the operational results they were going to have would stretch far beyond Norway, and far beyond the North Sea.

Radio Deception and Codebreaking in the Invasion of France

In World War I, the French army had used a four-digit cipher based upon a codebook that contained 10,000 letter groups which offered a way of enciphering every conceivable type of military instruction or activity. The code was overwritten with what was called a 'finite addition cipher'. Thus letters and numbers could be inserted at the beginning, in the middle or at the end of the figures or letters that contained the actual message. The French made the mistake of not changing the addition ciphers frequently, so in the 1930s the Germans, over a period of time and from comparison of numerous messages, worked out which letters or numbers belonged to the addition ciphers. These varied between seven and thirty-one digits and letters. For Erich Hüttenhain it was easy: the messages enciphered with this cryptograph were entirely read by the OKW-Chi in the last years before World War II. And in February 1940, OKW-Chi intercepted just two of thousands of messages coming from the French army the other side of the Maginot Line, a defensive, fortified barrier erected on the French borders with Germany, Italy, Luxembourg and Switzerland. It was made up of fortifications and weapons emplacements, with living quarters for troops, a small railway inside some of the installations that could move food and men and ammunition around quickly, and heavy guns that covered arcs of movement in terrain where the French thought a German assault was likely to come. The line did not extend to the Channel in its northern sector, as the British and the French both expected to be able to move into Belgium to counter-attack, while the Maginot Line itself would hold up the Germans long enough for Allied forces to consolidate and attack.

When studying the gathered material of cipher texts, two messages were found that had large and long sequences of almost identical numbers in them. The only thing that was different was the sequence of digits in the first two lines. The canny former astronomer Hüttenhain saw that what was in front of him was a substitution process overwritten with a transposition process, or a

Würfel, meaning 'matrix' or 'cube'. The numbers or letters would be rearranged using a simple substitution process, and then sections of the coded text would be transposed, and swapped around in a different running order. Hüttenhain saw that the substitution key was a four-digit code. It turned out that in the two messages that led to the break-in of the system, there was an identical longer passage over several lines of the messages. It was another example of a parallel text compromise. Going further than this, he saw that both the code and the key to which sections of text should be transposed were linked. Uncoded sections of the text contained the transposition keys. So if a message said '*IV Army movements to Alsace from Italian border Savoie due 11th August without replacement*', one of the words in the message – 'without' – would contain the transposition codes. With seven letters in the word 'without', it would mean that every seventh section of the coded text would be moved by seven figure places, seven times, until the next transposition code letter was introduced. Knowing what the transposition key was also helped reconstruct and recognize new code groups. Hüttenhain said:

> We called it the 4ZCüWü. By mid-1939 the entire communication traffic of 4ZCüWü, a 4-digit code overwritten with Würfel, between the French Ministry of War and the Wehrkreis [defensive circle] bordering Italy was read. When the war with France broke out on September 3, 1939, the French ministry of war ordered the use of 4ZCüWü for all other Wehrkreise as well. The code remained the same, they only made minor changes at the first of each month to the Kenngruppe [the indicator key]. These changes were quickly recognized and after a few times even anticipated. This remained until the end of the French campaign, every message was read by the German side, the German military leaders were always informed of all essential operations of the French army: the read messages not only informed about the structure of the French army but also about the armament of the individual units, the weakest spot of the Maginot line, the atmosphere and attitude of the troops and among the people of France and in the colonies. The information also included the deployment of British troops on the continent and their movement.[2]

When the Blitzkrieg unrolled, what OKW-Chi would learn from the French army codes also included large amounts of information about the operational

activities of the British Expeditionary Force (BEF). Firstly, they discovered that the RAF was desperately short on fuel and wanted to conserve its aircraft for the defence of mainland Britain. Secondly, the Germans discovered from reading French and British signals that the BEF would not fight to the death to protect France, but would stage an evacuation mission if necessary. The Germans could read the French navy, army and air force's main ciphering systems, and had particular successes – as Hüttenhain demonstrated – with the codes of the French war ministry, a four-figure codebook of 10,000 groups enciphered with additive sequences.

Wilhelm Fenner at OKW-Chi, who was of course Hüttenhain's civilian manager, said this:

> Even before the military action with France began, the military systems of French higher staffs were solved. This was a 4- or 5-figure code that was systematically transposed [tableau carve]. In the cryptograms a few parallel passages [repetitions] were discovered. The interval between these passages was constant and must therefore correspond to the width of the transposition box as cryptanalytic studies have shown. If I am not mistaken the keys for the box itself were taken from the same code book. Despite all the cunning of this cryptographic system, the occurrence of short parallel passages proved fatal. By the aid of these deciphered messages tabs could be kept on the French Army far back into the homeland.[3]

Ferdinand Feichtner from the Luftwaffe's signals intelligence was by now an officer, and he too had been busy. Listening stations on the French border with Germany were intercepting a large amount of radio traffic from French fighter aircraft patrolling the airspace over the frontier. Seeing immediately that the French pilots were obviously communicating with each other, Feichtner worked out, from a captured handbook of the French air force, or *Armée de l'Air*, what kind of radios the French were using. He then made sure that the section of French-speaking personnel who specialized in radio direction-finding were sent to two monitoring stations near the French border. The pilots' radio discipline, the Germans discovered, was almost non-existent. So each time a French fighter patrol took off to patrol the frontier area, pre-arranged radio contacts between Feichtner's listening station and German fighter bases were activated. What this meant was that when the

listening station knew that French aircraft were about to take off, or had taken off, German fighters could scramble to meet them, knowing exactly where they were.

The Germans Deceive the French

In October 1939, a German colonel called Kunibert Randewig of the army's signals corps was told to prepare a wireless deception plan by Major General Fritz Thiele, the chief signals officer to the Heer.[4] Randewig was responsible for three signal intercept companies posted to monitor Germany's western border, as, after the outbreak of war, Germany initially thought France might try to invade Germany. The planning for this deception scheme against the French took place between October 1939 and February 1940, and Randewig was told to work out details with the chief signals officer of Army Group C. The initial plan involved persuading French military intelligence to believe that a new, but in reality entirely fictitious German army of ten divisions, or three corps, was being moved into a position on the Siegfried Line between the 2nd and 7th German Armies. The plan was to make the French retain their strategic reserve in the area around the cities of Nancy and Metz in eastern France, and try to make them believe that a main German attack was imminent on the Maginot Line. The Germans were convinced that an early move by these French reserves might constitute a major threat to the German left flank during the planned invasion of western Europe.

Oberst Randewig thought, however, that because there were ample phone line communications in the area where this fake army was to be situated, the French would easily work out that the entire plan was a clever intelligence ruse. However, to maintain the deception, the Germans decided that only their training units in the area east of the Lower Middle Rhine and the Black Forest would be allowed to use radios. Indeed, the plan was to have radio silence on the front line, but in comparison a large volume of traffic in training areas in the east, so the French were convinced that a large formation was on its way to the front. Signals would have to be sent on wavelengths on which the Germans knew the French would be concentrating their direction-finding effort, and on radio sets strong enough to reach from German training areas to France. Just before 10 May, which was earmarked as invasion day, the 'fake' army would then turn off its radio signals so the French believed it was moving onto its operational area. The concentration

area for this non-existent unit and its non-existent training was in western Germany, between Grunstadt and Bad Durkheim. Bogus wireless traffic was to begin on 5 May, imaginary railway journey links were invented, and this fake wireless traffic of an invented army on the move on roads and railways would be transmitted in an international code used by the German Post Office and Police. The messages about road movements were so poorly encyphered that it was assumed that even French radio operators of low skills could intercept them and decrypt them. Since a civilian net would be used to broadcast these messages it was assumed that no breaches of security would be picked up by the German army, and finally, during the move of the imaginary army mention would be made of towns and areas of the training ground from which it had come. Deliberate breaches of security were also encouraged – private conversations between radio operators let slip such details as unit movements by this phantom army towards the new front line. It was a hugely ambitious and imaginary plan, and the Germans had high hopes that it would prove effective.

Yet some months prior to this, on 10 January 1940, reality and deception had unexpectedly crossed. A German Junkers Ju 52 transport aircraft had been obliged to make a forced landing near the town of Mechelen in Belgium, and the Belgians captured the pilot, crew and a Wehrmacht staff officer travelling on board carrying a full set of documents for the actual invasion of France. But the Belgians – and the British, to whom they passed the maps and plans – thought this was too good to be true, and doubted the plans were genuine, thinking they were a deliberate piece of deception. The British and the French were firmly convinced an attack would come directly on the Maginot Line, and they even suspected the Germans might invade Switzerland as well. What they did not foresee was a German assault through the Ardennes, as laid out in the captured plans carried by the German officer travelling on the downed Junkers. Indeed, such was the firm belief in the theory of an attack on the Maginot Line that the Allies simply couldn't believe the true German strategic planning when they saw it. The joint German deception plan organized by the Wehrmacht and by OKW-Chi thus turned out to be highly effective.

The Belgians thought – correctly – that the Germans would attack through the Ardennes, and try and land paratroopers to capture Belgian fortified positions. This strategic anticipation was backed up by intelligence reports received from a variety of their allies, which in turn were being intercepted by

German codebreakers from OKW-Chi and Pers-Z. Because Erich Hüttenhain had cracked into the French military field code, he could follow the information trail of which parts of the Germans' real plans, and their elaborately-staged deceptions, the Belgians were reporting to the French Ministry of Defence and vice versa**.**

So when, in March 1940, Swiss military intelligence noticed a build-up of German armoured units on the joint borders of Germany, Belgium and Luxembourg, they sent a signal to their own ministry of foreign affairs stating that up to eight German Panzer divisions had been observed moving in the area. Pers-Z's cryptanalysts were reading some messages enciphered by the Swiss on their Enigma machines and so intercepted and read this signal. The jigsaw of information then got larger: French military intelligence were then told by their own agents in Luxembourg that the Germans were building pontoon bridges over the River Our, which sits on the border of Germany and Luxembourg. The same source reported that in Germany there seemed to be a continuous column of German armoured vehicles, lorries and horse-drawn transport. OKW-Chi subsequently read both transmissions, and then on 30 April, ten days before the planned invasion day, Wilhelm Fenner's teams intercepted a message from the French military attaché in Bern, the Swiss capital. The Germans, it said, would attack at Sedan on the River Meuse.

The Fall of France

When the invasion finally came on 10 May, it lasted six weeks. It involved 157 German divisions, with 2,439 tanks, and 7,378 guns, anti-tank and artillery pieces. Of this enormous army, only a tenth was mechanized, most relying on horse-drawn transport, while nearly 45 per cent of the men were at least forty, and half of them had only two months' training; but the *Blitzkrieg* plan worked like a tropical storm against a town made of cardboard houses. German radio communications between the Luftwaffe and ground units was highly effective; the Panzer-led mobile warfare outstripped the French and the British with its speed. The German invasion of France had involved two main operations. *Fall Gelb*, or Case Yellow, saw German armoured units push through the Ardennes and then along the Somme valley, cutting off and surrounding the Allied units that had advanced into Belgium to meet the expected German invasion. When British, Belgian and French forces were

pushed back to the sea by the mobile and well-organized German operation, the British evacuated the BEF and several French divisions from Dunkirk in Operation *Dynamo*. After the withdrawal of the BEF, the German forces began *Fall Rot*, Case Red, on 5 June. There were sixty remaining French divisions which put up a determined resistance, but were unable to overcome the German air superiority and armoured mobility. German tanks outflanked the Maginot Line and pushed deep into France. German forces occupied Paris unopposed on 14 June after a chaotic period of flight by the French government that led to a collapse of the French army. German commanders met with French officials on 18 June with the goal of forcing the new French government to accept an armistice that amounted to surrender. On 22 June the Second Armistice was signed at Compiègne by France and Germany. This resulted in France being divided, so that the centre and south was controlled by the neutral Vichy government, while the north and west was occupied by the Germans.

Chapter Nine

FIGHTING THE WAR IN THE AIR

The Codes of 'The Few'

One night early in October 1939, a British Wellington bomber was flying over Erfurt in central Germany, on its way back from a mission. A Luftwaffe anti-aircraft unit spotted the aircraft and opened fire; it crashed in flames. When the fire had died down, and German troops searched the radio operator's position in the fuselage, they found a series of cards. These had random characters printed on them, in lists that ran horizontally and vertically: the soldiers who searched the wreckage thought they might be important, and handed them to their unit commander, who in turn gave them to his intelligence officer. They eventually reached the cipher bureau of the Luftwaffe's OKL Chi-Stelle, and landed in front of the German cryptanalyst Ferdinand Voegele, a linguist and philological expert.[1] He recognized them: they were lists of daily codes for the British Syko encryption machine used by the Royal Air Force. This replaced letters and numbers with other letters and other numbers, chosen seemingly at random, and every twelve hours the card was changed, so the British assumed it was impossible to break into the code. It was, unless the enemy cryptanalyst had a series of captured Syko cards in front of him, and had also been able to intercept the radio messages over the preceding twelve hours that were encrypted using that day's Syko card. By that point in 1940, the Luftwaffe's cryptanalysts could do

both. In the preparation for the forthcoming invasion of Europe, they were working as hard as they could to break into the RAF's codes.

Voegele was forty-four that year, and came from Bavaria. During World War I he had volunteered as a radio technician, and had then studied Oriental languages and worked for an export business, before becoming, in the summer of 1935, an interpreter with the German air ministry. He trained in Morse telegraphy and cryptographic procedures, after which he was posted to an army intercept station near Stuttgart in 1936. He translated plain text messages from the French army and air force, and also spent two months airborne, working in a Luftwaffe intercept aircraft as a radio operator. The next stop was Munich, and an intercept station translating French, Italian and Serbo-Croat. He was one of a professional type that had been increasingly recruited into the world of cryptanalysis prior to the outbreak of war. The linguists, professional interpreters, mathematicians, logicians, electronics experts and radio specialists were the new avant-garde in a world of covert communications that was evolving and developing as rapidly as the movements of the troops, ships and aeroplanes it monitored. The side that moved faster and more skilfully, while evolving and adapting to its enemy's quickly expanding technological skills, would be the one that would win the day. Yet as with any technical or personnel intelligence asset, its tactical and strategic usefulness and effectiveness was only commensurate with the ability of its handlers to put this intelligence into operational practice. It was a huge leap reading into the enemy's bomber codes, but if your own side did not have the aircraft or flak guns to shoot down the bombers or destroy their home air bases the information was worthless. It was the tried and trusted old saw of intelligence and active operations that had held good since man first went to war against man.

On New Year's Day 1937, the mousy and studious Voegele had been sent to the Luftwaffe's newly created cipher bureau and given command of it. He had an assistant, who handled cryptanalysis of Russian army codes, and eleven other colleagues. Voegele was a happy man: he liked what he did, cooperated with his colleagues, had no particular liking or dislike for National Socialism, and was even-tempered and very curious. He made the perfect cryptanalyst, a type described as 'Beethoven with the soul of an accountant'.[2]

'In the Luftwaffe, Voegele was the outstanding man,' said OKW-Chi staff analyst Dr Franz Weisser. 'He lived an irregular life, but he was a hard worker notwithstanding … he was in my opinion better than Hüttenhain because he

had the real feeling for this matter. He did the work himself.'[3]

Voegele had worked on some of the Spanish Republican codes that Ferdinand Feichtner and his team were sending him from the Spanish Civil War, and tried to concentrate on deciphering the signals of Czechslovakia prior to the outbreak of war. His main priority, though, was the British Royal Air Force, and their four-digit RAF Code, their Aircraft Movement Code, and their Bomber Code. Everybody said the British air force codes were undecipherable, but Voegele disagreed: anything made by man could be undone by man. It was simply a question of finding a crib, a way of somersaulting into the code. He only had four cryptanalysts available for work on French, British, Spanish and Italian codes by winter 1939, and he didn't think any of them were capable. He needed more manpower.

General Wolfgang Martini, commander of the Luftwaffe signals corps, came to the rescue and sent him fifty men from the army signals units, who could help him go through the permutations of letter groups in the RAF four-figure code. Voegele had asked Wilhelm Tranow if he could send him any work he had done on the British Government Telegraph Code, as he suspected that the layout of the two four-digit codes, enciphered on subtractor tables, were very similar. The men that Martini had sent him were put to work as a form of human 'bombe', writing down every possible permutation they could think of that fitted in with the available intercepted RAF signals, and the few words they had that might act as cribs.* It was one of Voegele's Luftwaffe colleagues, however, that helped him make the first real progress.

Erich Hübner had been a glassblower's apprentice before he joined the signals corps in World War I.[4] His first unit commander was then-Captain Heinz Guderian, who would go on to be Germany's leading tank commander. Hübner was first a radio operator, and then a signals analyst; after the war he worked in journalism and as a bank manager, and then joined the Luftwaffe. 1938 saw him sent to the Balearic Islands, as part of the German signals monitoring team from the Condor Legion; he was based in Mallorca, which seemed a very long way from the chill winters of central Germany. The British and French were transferring aircraft to and from North Africa, as they manoeuvred their air force units in a cautious dance around the war in Spain. Both sides knew that they wouldn't get directly involved in the fighting, but everybody could see wider conflict coming across

the horizon, and Paris and London wanted their aircraft prepared, and in the right place. Their frequent signals gave Hübner and his men plenty of material, especially as mutual misunderstandings between signals sent in two languages meant that the RAF and their French allies often had to repeat the message, meaning that Hübner and his men immediately had examples of parallel text compromises from which to work.

Returning to Germany from Mallorca, he and his fellow Luftwaffe cryptanalysts continued to work on the Royal Air Force Code. Hübner saw that every month in England the RAF published what was called the Air Force List, available in London bookshops. While it didn't include the technical specifications of British aircraft, like speed and armaments and rate of climb or fuel consumption, what it did include was the registration number and name of each aircraft the RAF had. If the Luftwaffe signals intelligence men concentrated on intercepting messages from training flights across the Channel, they could start building up a picture of what type of aeroplanes the British had, where they were based and what they did. This would mean that the Germans would be able to work out some of the words in each message sent in the RAF Code. Hübner later recalled an example of how this could be achieved.

The RAF used a single-engine bomber called a Fairey Battle. With a crew of three, only two machine guns as defensive armament, and a speed of 100 miles per hour less than the Messerschmitt Bf 109, it was outclassed and obsolete by the time war broke out. Ironically, though, the RAF's first aerial victory came in September 1939 when the rear-gunner in a Battle shot down a Messerschmitt Bf 109 over Aachen. During the 'Twilight War', ten squadrons of Battles were sent to France to support the British Expeditionary Force. Other units remained in England on training missions. Hübner saw that the RAF frequently sent messages like this one: '*K7954 Battle with PO E.C Maxwell left Bircham Newton 0900 sta Turneridge 1030-0910.*'

Bircham Newton was an RAF base in Norfolk: the Air Force List gave the type of plane and its home base. So if the original message above was sent in the RAF Code, Hübner, Voegele and their colleagues now had at least one crib word: Battle. If they then went through the Air Force List they would see that two squadrons of Fairey Battles were based at Bircham Newton. This gave them two extra crib words for 'Bircham' and 'Newton'. Given that these were not commonly used words in the English language, it would be simple to spot their coded recurrence in messages. The plane's registration numbers

provided another numerical crib: if two Fairey Battles had registration numbers K7801 and another K8050, it was logical that every aircraft number in between was a Battle. Firstly, this told the Germans how many bombers of a particular type the British had, and secondly, told them that every message that mentioned a Battle and its registration number would immediately cross-reference to one of a series of squadrons in Britain or France. If two Battles code-numbered K7954 and K7964 were both based at Bircham Newton, it meant that each aircraft registration number in between 54 and 64 belonged to the same squadron. Knowing that there were twelve Battles in a squadron, this meant the Germans had a crib into every number in the RAF Code from 54 to 64, so 1, 2, 3, 4, 5, 6, 7, 8, 9 and 0. In this way, Voegele, Hübner and the Luftwaffe cryptanalysts began building up a picture of how many aircraft the RAF had, of what type and where they were based.

The second language crib that the Germans used was RAF weather reports: these were sent sometimes twice a day, detailing wind speed, cloud cover, external temperature at ground level and at 5,000 and 10,000 feet, rain or sun, and any specific predictions such as thunderstorms or periods of extended sunshine. These were sent in a five-figure weather code based upon subtractor tables that was very similar to the RAF Code. The very limited word selection used meant that repetitions and parallel texts were common. Given the breaks into the two different codes, it meant that by early 1940 the Germans could read into the RAF's Syko Code.

Progress was helped by the arrival of additional staff: Voegele's department had a fluctuating staff of fifteen to thirty people available for all foreign codes by the end of September, and by December this was fifty. This meant that by January and February 1940 Syko messages sent by RAF bombers were being intercepted at the rate of 300 per day, and this depth enabled the Germans to begin reading into their first message of the day by as early as 2pm. Voegele made a lengthy entry into his diary as to how he did this. Like the diary kept by Walter Fricke at OKW-Chi, it was irregular and forbidden, but Voegele eschewed discipline when it helped him do his job better, and anyway, he thought the rigid Prussian standards of the German Wehrmacht were the antithesis of the liberal and curious intellectual spirit that he saw as the basis of good cryptanalysis. In the diary entry below, he explained the method of decrypting four-figure codes using the non-carrying subtraction process, which was identical to that used by Wilhelm Tranow with British Royal Navy codes:

> At the end of October, 1939, I began statistics of RAF 4 fig. on messages of Oct. 39 with a group of 20 soldiers who had not the slightest idea about decrypting – there was no time for teaching. Four weeks later I had the first items – 2222 take-part 2, 1111, main code, 1584 from a.s.o. Shifting from relative numbers – for 2222 I had 9711 – 1111 was 0822 was done by 0983 = read following 5 figures in clear. I knew that the first digits of old non-comm. officers' Pay Book was 5 or 6, so I got the 5, the other digits I got by filling up figures with 000 for instance 0983 57643000. As a proof I found 5 messages dated December 24th (Xmas) which were sent in open code without recyphering. Further I got 2 messages sent in syko and repeated in RAF 4 fig. At the end of '40 some recyphering tables were completely reconstructed – 100 pages, each 20 lines, each line with five 4 fig. groups. In winter 1939/40 about 30% of these 4 fig. messages began with 2222. In January '41 many of the messages began with the text followed by address in brackets – so it was easier to find overlapping messages.[5]

Thanks to the repeated depths and the heavy RAF traffic of up to 600 messages a day, the skill in interception and decryption traffic analysis enabled the Chi-Stelle to break into and read, or understand, radio traffic, radio signals from radar and the deployments of both bombers and fighters across Great Britain.

On 18 December 1939, twenty-four RAF Wellington bombers flew to Wilhelmshaven on the German North Sea coast, their target a flotilla of naval ships in the harbour. En route, two radar stations intercepted them, and their radio signals announcing their flight progress – 'crossing enemy coast' – were intercepted and read by Luftwaffe signals intelligence crews. Wilhelmshaven was one of the continent's most heavily defended targets, along with Berlin, Vienna and the Ploiesti oil fields in Romania. Flak crews and fighters waited for the Wellingtons. Twelve out of the twenty-four bombers were shot down: it was a triumphant vindication for the Luftwaffe's new signals intelligence infrastructure.

The Battle of Britain, however, was not. The Germans had developed the means to monitor, intercept, decipher and take action on the more important of the Royal Air Force's operational codes. Yet this did not mean they had better aircraft than the RAF, better pilots or better strategy. In theory,

knowing what the British were going to do in advance, or as they were doing it, should have given the Germans a keen tactical edge. The Chi-Stelle by now had twenty-four mobile and fixed listening stations in Europe, and the closest one, near the Pas de Calais, established after the fall of France, was only forty miles from Folkestone in Kent. The December 1939 raid on Wilhelmshaven had shown how effective was their equipment, and they knew most of the operational strength of the RAF, and where its fighters and bombers were based. So surely it should have been able to achieve a tactical and strategic victory over the RAF in the months between June and September 1940? In theory, yes. In practice, no.

Germany's signals intelligence infrastructure was an essentially defensive invention, designed to pick up signs of incoming British fighters and bombers approaching Germany, and used as part of an integrated network of radar stations, monitoring bases and cryptanalysis. The last of these, importantly, took time: in the fastest case scenario a signal in the RAF Code about an imminent bomber mission could be intercepted at 8am, read at 8.15am, teleprinted from, say, Asnières outside Paris to Potsdam at 8.35am, received at 9am, passed to two cryptanalysts at 9.15am, and decrypted by 12.30pm. A squadron of Wellingtons that took off at 11pm from an RAF base in Cambridgeshire, for a night-time bombing run on the Ruhr,would be over the target by 1.30am, nearly twelve hours after the decrypted message had reached night-fighter and flak bases. It was totally the opposite in the case of offensive operations against England: by the time the Luftwaffe had picked up the RAF's signals announcing a squadron 'scramble' at Tangmere or Biggin Hill, the fastest speed at which it could be decrypted would mean that the RAF fighters would be attacking German bombers while Ferdinand Voegele's men were still subtracting four-figure letter groups from key words in the encipherment table they had so carefully reconstructed. The strategic impact of breaking the RAF's codes was substantial: they had an important role in helping the Germans intercept British bombers and fighters attacking across the Channel, but little impact on the outcome of the Battle of Britain, which was essentially an offensive operation for the Luftwaffe.

Winning and Losing the Battle of Britain

The Battle of Britain was won by the British and lost by the Germans for a number of reasons. The key factors briefly outlined below help to explain why

some of the most advanced codebreaking, and codebreakers, of World War II could not help Germany win the air war over southern England.

Firstly, Air Chief Marshal Hugh Dowding, the head of Fighter Command of the Royal Air Force, was a vastly more competent leader and strategist than Hermann Göring. Like the Germans, the British could also rely on an excellent listening service. The radar station of the 'Chain Home' network and the men and women of the Royal Observer Corps gave the British ample warning time of incoming German aircraft which Dowding and his Group Commanders used to great effect when deploying their fighters.

Secondly, the British had produced very good fighter aircraft in the Hurricane and the Spitfire. Furthermore, the British and Commonwealth pilots were well trained, defending their homeland, and if shot down tended to land in a hop field in Kent and not in enemy territory – they could fight another day. Their downed aircraft could be repaired and recovered out of the sight of the Germans even once shot down; so a damaged aeroplane was in fact a machine that could often be flying again a week later. The RAF could draw not only on British pilots but on Poles, Czechs, New Zealanders, Australians, Americans and South Africans, many of whom had previous flying experience. Certainly, the Spitfire and Hurricane individually could not always out-perform German aircraft like the Me-109, especially when flown by pilots with combat experience in Spain or Finland; but they could do so when collectively deployed with a mix of aircraft assets flying against both bombers and fighters. The eight .303 Browning machine guns mounted on Spitfires and Hurricanes sometimes meant a very high usage of ammunition to down one bomber, but some British pilots perfected head-on attack techniques that allowed them to maximize this firepower, and avoid the defensive weapons of German bombers, by flying straight at them. On 30 August Squadron Leader Tom Gleave of 253 Squadron shot down four Me-109s in the same dogfight using this tactic; the third and fourth German aircraft were only sixty and seventy-five yards away from him when he opened fire on them. Additionally, British fighters were flying against slower, more heavily laden German bombers operating in tight formation, which made them easier targets than individual fighters.

But for all the abilities of the RAF pilots and their aircraft, it was how they were skilfully deployed that ensured that throughout the summer of 1940 they remained unbeaten. In World War I Room 40 had been able to listen to the Kriegsmarine but were unable to have any operational outcome on the

battle. Here, there was a direct, positive operational impact that the German codebreakers, despite their successes, could do little to diffuse.

Indeed, unbeknown to Ferdinand Voegele and his teams of German air force codebreakers, the British were already reading messages encrypted in the Luftwaffe Enigma cipher. In the summer of 1940, British cryptanalysts at Bletchley Park were reading messages regarding everything from German troop movements to the assembly of barges; the Luftwaffe was instructed not to bomb English quays, which were to be used as debarkation points for the invading troops. By mid-July 'the Park' had even decoded a message from Göring informing his generals of Operation *Sealion*; and then the British decoded further messages, revealing squadron strengths and their locations in Holland, France and Belgium. By September 1940 the Germans had lost the aerial battle and so they resorted to a bombing campaign that was aimed at crippling Britain's wartime economy.

---

* The 'bombe' became the collective name for mechanical devices, such as the ones used at Bletchley Park, which were very early computer prototypes and could process vast amounts of data containing every single possible figure and letter permutation of the contents of signals in both plain and enciphered text.

Chapter Ten

THE BATTLE OF THE ATLANTIC

Diana and Hubertus in the First Happy Time

On 1 September 1939, Karl Dönitz, who was then a naval commodore, attended a meeting with Grand Admiral Erich Raeder, commander-in-chief of the Kriegsmarine. Based on his experience in World War I, Dönitz told him that with a fleet of 300 U-boats, he could wage a sea campaign that could cripple the British maritime supply lines, and its imperial economy. They could prevent supply convoys carrying food, armaments and crucial fuel from reaching Britain's shores. The problem was that Germany had only fifty-seven submarines at that point, and of them only twenty-seven were fit for service at sea. The absolute minimum that Dönitz needed was ninety operational U-boats, to be able even to begin to put his plan into action. Raeder and Dönitz both knew that Germany's naval rearmament plan was in full swing: another thirty new U-boats were scheduled to be launched by the end of the year. So Raeder instructed him to launch his campaign with the assets he had available. The Battle of the Atlantic had begun.

•••

On the same day, the passenger ship SS *Athenia* left Glasgow for Montreal. It was carrying 1,103 passengers, of whom some 500 were Jewish refugees, and

the remainder a mixture of Canadian, American and British citizens. It had on board a crew of 315. Its captain, like many others on both sides of the Atlantic, knew that war was going to break out at any moment, but regardless, it left Liverpool for the open Atlantic at lunchtime on 2 September. By the 3rd, it was 200 miles north-west of Ireland, and at 4.30pm Oberleutnant Fritz-Julius Lemp sighted it. He was the commander of U-30, a 600-ton Type VII-A U-boat that had been laid down and built as part of Plan Z, the secret German rearmament plan. Based out of Wilhelmshaven, it was sailing as part of the 2nd U-boat Flotilla, and had been at sea since 22 August, before war broke out. Lemp thought the darkened ship, which was sailing a zigzag course, was a troopship, an armed merchant cruiser, or a Q-Ship. These were merchant ships equipped with disguised or camouflaged guns, designed to lure U-boats into making attacks on the surface. So Lemp and U-30 followed the *Athenia* for three hours, before he gave the order to launch two twenty-one-inch torpedoes. One exploded on the ship's port side, inside its engine room. The ship started to go down at the stern. Lemp headed away at full submerged speed, while three British destroyers, a Norwegian tanker, a Swedish yacht and an American cargo ship rescued some 1,300 passengers and crew. A total of 118 people died.* Meanwhile, the German liner SS *Bremen*, sailing from New York to Murmansk, ignored the *Athenia*'s distress signal. The response from Britain and its allies to the sinking was outrage.

'Liner Athenia is torpedoed and sunk', ran the headline in the *Halifax Herald* in Canada on 4 September. In the centre of its front page was a red banner headline that said: 'Empire at war'.

When Grand Admiral Raeder first heard of the incident, he demanded to know what had happened. He quizzed his U-boat headquarters, who told him that no German submarine had been any closer than seventy miles to the *Athenia*. The German naval commander duly told the chargé d'affaires at the American embassy in Berlin that his men had not been responsible. The German Ministry for Propaganda even claimed that a British submarine had sunk the *Athenia*, so as to provoke the United States into joining the war. On returning to Germany, Oberleutnant Lemp reported to Dönitz that he had indeed sunk the *Athenia* by mistake, thinking it was a troopship. Dönitz sent Lemp to see Raeder, who then met with Hitler.

The Hague Convention Prize Rules stated at that point that the captain of a ship or submarine had first to get the passengers of a civilian ship into

lifeboats before sinking it. Dönitz's reaction was threefold: U-30's log was falsified, the Germans lied about the sinking, and until December 1939 captains were ordered to follow the Prize rules. Then before the end of the year, Dönitz's strategy changed, and became one of sinking as many ships as possible with or without their crews. He told his U-boat skippers 'rescue no one and take no one with you. Have no care for the ships' boats.'[1]

On 14 October 1939 Kapitänleutnant Günther Prien took the Type VIIB submarine U-47 through the booms and anti-submarine nets into the British Royal Navy's home anchorage at Scapa Flow in the Orkneys. Dönitz and Raeder had both decided that if they attacked the British Home Fleet at anchorage, they could force it to move elsewhere, away from Britain's eastern cost, and so give the Germans greater leeway to attack Atlantic convoys and avoid the North Sea blockade. The Royal Navy wanted to direct its Home Fleet of battleships, cruisers and destroyers into more offensive operations against submarines in the Atlantic; they found themselves in direct opposition to the army and the government who wanted the fleet deployed to protect ports in eastern and southern England against a possible invasion. Britain now had fewer naval assets in the Channel, meaning it had to divert more of its ships from Atlantic convoy escort duty to protecting ports. So Prien's attack was designed to disperse the Royal Navy's assets by proving that even in their home anchorage they were not safe against submarine attack.

Sailing on the surface, with his approach lit up by the glow of the northern night-time Aurora Borealis, and the headlights of a Scottish taxi that momentarily drove past on land, Günther Prien manoeuvred himself into Scapa Flow until he was diagonally lined up against the World War I-era battleship HMS *Royal Oak*. U-47 fired a spread of eight G-7a torpedoes at her. Of the first four from the bow tubes, one jammed in the launch tube, and two malfunctioned, due to problems with their depth steering and magnetic detonator systems. The G-7a torpedoes were powered by decaline, a fuel that burned in a combustion chamber and created steam from heating fresh water, which powered a small four-cylinder engine. The torpedo was equipped with a mechanical and magnetic exploder, which had not been tested before the war on 'live' targets, so it had a tendency to malfunction. But one of Prien's torpedoes hit the mark, running straight into the stern of the old battleship. As his men reloaded the bow tubes, Prien turned his boat around and fired another torpedo from its stern tube. This too missed. But with the bow tubes now reloaded, he fired another three, all of which hit the

Royal Oak. The explosions blew through its armoured deck and ignited cordite from one of its magazines. It turned over towards one side, listing; then went down into the shallow anchorage thirteen minutes after being hit. As it sank, the surface of the sea around it was instantly covered with a glutinous thick film of fuel oil. Many of the crew who jumped overboard were only wearing their nightclothes. The water was very cold, and as the men and boys from the ship tried to swim the half-mile to shore, the clogging oil filled their lungs and stomachs as they both swam and tried to breathe simultaneously. Many didn't make it to shore. 833 people died, of whom more than 100 were boy sailors, under the age of eighteen. Prien and U-47 returned home to an instant hero's welcome, and the submarine commander received a Knight's Cross of the Iron Cross from a delighted Hitler.

That autumn, two other U-boat attacks also had an immediate and influential impact on the operations of British ships in the Atlantic: on 14 September a U-boat scored a near-miss on the carrier HMS *Ark Royal,* while on 17 September a U-boat sank the British aircraft carrier HMS *Courageous* off Ireland. As a result the British Admiralty decided that carrier-based anti-submarine patrols were too risky to valuable ships such as *Ark Royal*.

By the following summer, France had fallen and the Battle of Britain was in full swing. German U-boats could now operate from bases on the Atlantic coast of western France, and between July and October 1940 more than 260 Allied and neutral ships were sunk in waters off Britain and in the Atlantic Ocean. As this rate of sinkings continued, U-boat crews started calling their successes against Allied shipping '*Die Glückliche Zeit*', or 'The Happy Time'.[†]

In seven days in July, the rate of sinkings, the Allied naval counter-attacks against U-boats, and the range of international shipping being attacked showed something of the fast-moving ferocity of the opening days of this phase. It was the opening of a battle whose field would be the vast, heaving, dark and merciless waters of the North Atlantic, which above the equator covered more than sixteen million square miles between Europe and Africa – the Old World – and the United States, the New World. The waters were deep, with a range of around 12,000 feet in many places. The ocean was huge, and for both the Germans and the Allies a major part of any offensive or defensive action between U-boats, Allied supply convoys and their naval escorts consisted of simply finding the enemy. This was one fundamental reason why radio communication, coded or otherwise, was so vital. Destroyers and corvettes had to find and track submarines, who in turn had

to locate convoys, who themselves tried to evade the attack lines set up by the U-boat 'wolfpacks'. Merchant ships, submarines and escort vessels relied on radio communication to tell each other where the opposing side was, wasn't, could be, might be or had been. The volume of radio traffic was thus vast, and it stood to reason that if either or both sides could read the encoded signals the other was transmitting, the tactical and strategic advantage thus gained would be crucial, and would make the difference between defeat and victory. Yet in the battle's opening phase, much of the action was centred on the sea lanes west of Ireland, Scotland and Land's End. U-boats attacked merchant shipping of any nationality bound to and from the British Isles, and the list of those sunk or damaged in one week gives some idea of the intensity of the opening stages of the battle.

On 1 July, at 4am, 300 miles west of Brest, U-30 sank the British merchant ship SS *Beignon*, sailing in convoy, and U-102 sank the SS *Clearton*. In turn, the British destroyer HMS *Vansittart* found the U-102 with its Asdic sonar-detecting device and sank it with depth charges. Meanwhile, U-65 sank the Dutch freighter *Amstelland* and U-29 torpedoed the Greek ship *Adamastos*, while off Ireland U-26 damaged the British ship *Zarian*, before the Flower-class corvette HMS *Gladiolus* depth-charged U-26, and then a Sunderland flying boat crewed by Australians from the Royal Australian Air Force bombed her.

On the 5th, U-34 sank the British destroyer HMS *Whirlwind* off Land's End, while U-99 torpedoed the Canadian merchant ship *Magog*, blowing it in two. The stern of the ship went down immediately into the Atlantic, but the front kept afloat as the ship was carrying a huge load of timber, allowing its crew to be rescued. On the 6th, U-34 sank the *Vapper*, an Estonian ship carrying coal, while south of it Fritz-Julius Lemp in U-30 – by now promoted to Kapitänleutnant – sank the Egyptian freighter *Angele Mabro*. The 7th saw U-99 sink the British MV *Sea Glory*, and then the Swedish SS *Bissen* off Cape Clear, as U-34 torpedoed the Dutch tanker *Lucrecia*.

U-34, commanded by Kapitänleutnant Wilhelm Rollmann, was on its seventh patrol by the time July 1940 turned. The boat had already served in the Spanish Civil War, where it had sunk a Republican submarine, and between September 1939 and 1 August 1940, the Type VIIa submarine sank nearly 100,000 tons of Allied shipping, including twenty merchantmen, two Allied escort vessels and a Royal Navy submarine.

U-99, meanwhile, was captained by one of Germany's submarine heroes,

Otto Kretschmer, who became Germany's most successful U-boat commander of the war, sinking shipping totalling over a quarter of a million tons. Kretschmer was noted for his humane treatment of survivors of his attacks. Several merchant seamen described the aftermath of being torpedoed by U-99. Once they had jumped overboard, or taken to the lifeboats, sailors from Kretschmer's submarine had passed down tins of biscuits or bottles of spirits to the sodden, freezing sailors.[‡] Kretschmer was known as 'Silent Otto', both for his reluctance to broadcast any unnecessary radio messages while on operational patrols, and for his 'silent running' attack techniques. He would steer into the middle of convoys, at night, on the surface, trying to use only one torpedo for each of his targets. The British thought his bravery quasi-insane.

After he had torpedoed the British merchant vessel *Humber Arm* at 7.57am on 8 July, he found himself under heavy attack by British escorts, who hurled 104 separate depth charges into the sea around his boat for fourteen hours. Depth charges were dropped into the water at places where convoy escort vessels thought submarines were moving. As the U-boat moved into or out of its attack run, it was at most risk of being located by Asdic, HF/DF ('Huff-Duff')[§] or visual sighting. The escort vessel would roll the drum-shaped device off the stern of the ship, or fire it from launchers. Carrying 300 pounds of Amatol explosive, the charge was designed to submit submarines to a powerful hydraulic shock, with a fuse that was set for specific depths. Some sailors added hundred-pound iron weights to the depth charges to make them sink more quickly. If they exploded at twenty feet or less from the submarine's pressure hull, they would split it, and at forty feet, the blast would force the U-boat to the surface. The depth charges could explode at up to 900 feet below the surface, but launching them and achieving a successful strike on a submarine was very difficult: the escort vessel needed to move away from the blast area; the rolling, heaving Atlantic meant that the submerged U-boat was shifting upwards, diagonally, sideways and downwards in a three-dimensional watery matrix; the depth charge fell at eight feet per second; and a submarine could survive multiple blasts if the depth charges were not close enough.[‖‖]

Admiral Dönitz's Submarine Command

The German invasion of France had immediate tactical and strategic results

for the U-boat service. One of the most important was that they could establish submarine bases on the Atlantic coast. The U-boats in, say, St Nazaire on the west coast of France were then positioned at least 800 miles closer to the Atlantic than they would have been in Kiel or Wilhelmshaven. In addition, it meant that they did not have to run the Royal Navy's Channel gauntlet to get to the convoy shipping lanes, or execute the long, fuel-consuming trip around the north of the Orkneys, through the Faroes and Iceland. The first U-boat bases were established at Lorient, Brest and at La Pallice, the deep-water port of La Rochelle. Dönitz proved to be an officer who commanded his men from the top, often in person, and closely. His first operational headquarters was at Villa Kerillon, a large square building constructed in the nineteenth century, set on the bay at Port Kernevel, outside Lorient. A garden wall surrounded the villa, and in the lee of this was built a series of bombproof concrete bunkers from whose terraced roofs Dönitz would wave and greet departing or returning U-boats. These would dock into the submarine pens at the naval base, sitting across the bay on the Keroman peninsula; this became the largest and most heavily fortified German armed forces construction outside of Germany itself. With twenty-one feet of concrete above the pens themselves, Keroman was to earn the reputation as one of the four most-bombed sites in Europe, along with Berlin, Kiel and the Ruhr armaments factories. Dönitz decided to build the base at the end of June 1940, and three enormous structures of steel-reinforced concrete, capable of housing thirty U-boats, were constructed.

U-boat captains leaving on and returning from patrols had to make prompt and accurate reports to Dönitz, in person. When at sea a strict programme of radio silence was observed at certain points, as when going into an attack on a convoy or escort ship, but during combat patrols Dönitz wanted a constant flow of information from his submarine captains. As the U-boats surfaced and dived constantly, signals encoded on Enigma would be sent from the bunker outside his headquarters at Villa Kerillon, and their transmission repeated every two, six, twelve and twenty hours until the U-boats acknowledged. The first message would be sent from Lorient and then from the huge radio transmitter at St Assise, south-east of Paris, formerly the transmissions hub of the French Colonial Office. Built in 1921 by the Radio France company, the eleven pylons and five masts that reached up to 750 feet into the sky were behind what was then the most powerful radio transmitter in the world; by 1925, short-wave transmissions from St Assise had reached

Indochina.

Dönitz commanded by maintaining personal communications with his U-boats; he followed the progress of each of his boats on each patrol one by one. He held daily briefings where half-a-dozen deputies and staff officers received their orders. Enigma was then used to turn these orders into signals for the U-boats out at sea. Fifteen to twenty Kriegsmarine radiomen worked in shifts: the four inner rotor settings on the naval Enigma M4 were changed, by officers only, every forty-eight hours. The two outer were changed every day by non-commissioned officers or other ranks every day. Once the officer of the day had changed the inner settings, another officer inspected them. Similarly with the outer rotors: a different sailor inspected them every day.

Each U-boat had two radio nets, each with six frequencies, and the two nets were codenamed 'Hubertus' and 'Diana'. St Hubertus was the patron saint of hunters. He lived in the sixth and seventh century, and after his wife died in childbirth, he is reputed to have given himself up entirely to hunting in the Ardennes. One Good Friday morning, when everybody else was in church, Hubertus went hunting. He was chasing a large stag which suddenly paused in its flight, and turned to him, showing a crucifix glowing between its antlers; Hubertus put down his bow. Afterwards, he left him to find his way out of the forest, and embraced a saintly lifestyle which resulted in his eventual canonization. Diana, meanwhile, was the Roman goddess of hunting, nature, moonlight and animals. So the U-boats, out on their maritime patrols under the endless stars and thunderclouds of the North Atlantic, communicated through the saints and gods of hunting and animals. Not for nothing did some U-boats tend to have an emblem of an animal painted on the side of their conning tower. This was a habit that started with Günther Prien's U-47, when, after the successful sinking of the *Royal Oak*, the crew painted a snorting bull's head on their boat.

Using the Enigma machine, radio transmission was a very precise process. For instance, if Dönitz or one of his staff officers wanted to send a message to U-703, operating out in the Atlantic west of Greenland with the wolfpack codenamed *Stauchritter* (Bush Knight), this is how they did it. The daily officer of the watch at Lorient would take the message dictated by Dönitz or one of his subordinates, timestamp it, and give it to the duty radio technician watch officer for encryption. He would be just one of the fifteen to twenty radiomen who worked each shift enciphering and deciphering messages. The officer of the watch, a position that rotated every day, would be the one

responsible for setting the rotor position on the Enigma machines that communicated with the U-boats' Diana and Hubertus radio nets. As explained, only officers could set the inner rotor positions; they did this every forty-eight hours just before midnight, leaving the second of the pair of 'duty' Enigma machines on the previous day's settings in case late messages arrived from U-boats which were still using the previous rotor settings.

After the officer had completed setting the rotors, the radio technician would configure the Enigma's plugboard and turn the rotors to the required key. When the Enigma was configured, the message would be enciphered, and then immediately deciphered on another Enigma machine to make sure that it could be read. If so, it would be transmitted. As the recipient of the signal was normally a submarine, the first thing the technician had to do was to find out where it was located. This in turn determined on which radio circuit the message was sent. There was Amerika A, for the northern Atlantic, Amerika B for the southern Atlantic, Afrika 1 and 2, and three others. But submarines operational against convoys used Diana and Hubertus. The former had three different frequencies, and depending on the time of day and the local atmospheric receiving conditions, a different one would be tuned to receive signals from Lorient. Hubertus had six different frequencies.

The duty radioman at Lorient would then transmit the message in Morse code to St Assise, which in turn would transmit the signals at pre-determined intervals of two, six, twelve and twenty-four hours. If they were urgent, they were sent again two days later. There were six different categories of message. The first was called a 'long' signal. These were messages encoded into four-letter groups, such as MHEV, by the naval Enigma; the first two and last two groups were repeated indicators, which gave the recipient the different Enigma cipher being used, and the initial set-up of the rotors. The lengths of messages varied between around ten and eighty letter groups, which, at a rate of two-and-a-half seconds of Morse transmission time per group, would take from twenty-five seconds to three minutes to transmit in Morse. Of course, the longer the message, the better a target it made for interception, either by Allied direction-finding radar, or by HF/DF, or 'Huff-Duff'. To avoid sending long signals that devices such as Huff-Duff could track was one reason why the Germans preferred using the Enigma. It could condense relatively long messages into groups made up of four letters that could be sent very fast by a good Morse operator.

When an Allied convoy was sighted, the report was encrypted first by the

Signal Book of the German Navy, and then in the naval Enigma. After 1943 the Germans introduced the Short Signal Book, but the two procedures were essentially similar. The most urgent messages a U-boat could send, and the ones which carried the greatest implicit risk of their position being located, were convoy sighting reports, and reports that a U-boat was attacking or had attacked, or its particular location at sea. So these messages would be condensed into as short a signal space as possible in pre-coded groups. These were called Alpha messages, and were preceded by the German Morse code letter Alpha, whose aim was to clear the communications channel of less urgent messages. When it came to sending slightly longer messages, up to and including four groups of six letters each(so twenty-four letters in all), these short signals would be sent using the Short Signal Book for such reports as a convoy's speed and position, and the Short Weather Code Book for the routine weather reports that each submarine sent, giving details of prevailing conditions wherever it was. These messages would be preceded by the German Morse code letter Beta, and were thus called Beta signals. If there was a message of six four-letter groups, there would also be the five-letter message indicator, and the two-letter radio identification call-sign for each individual U-boat. The Short Weather Code Book contained letter groups, rather like a dictionary, that described every variation of longitude and latitude, atmospheric pressure, temperature, wind speed, cloud cover and visibility. The naval Enigma was then used to encrypt these. By the outbreak of war, submarines used a variety of fourteen Enigma keys, of which two of the most important were 'Freya', used by naval headquarters to communicate with its naval shore commands when landline telephones or teleprinters could not be used; and then 'Hydra', the main operational cipher used at the beginning of the war by all U-boats. This was also the main cipher used by German naval ships when they were operationally active in occupied territories. 'Medusa' was the primary cipher used by OKW to command and control all U-boats in the Mediterranean, and 'Neptune' the main primary cipher used by the German navy's capital ships. Lastly, and most importantly, was 'Triton', the cipher used by the German U-boat headquarters to all operational U-boats in the Atlantic. Of all the different Enigma keys, the three most important ones were 'Hydra', 'Medusa' and 'Triton'. And the last of these had even been given a special codename by British cryptanalysts, working at a country house north of London that the U-boat service didn't even know existed. The British Government Code and Cypher School at

Bletchley Park had their own name for 'Triton'; they called it 'Shark'.

---

* The Commonwealth War Graves Commission lists the number of *identified* casualties as 64.

† This became known as 'The First Happy Time'.

‡ It was apposite that when his U-boat was eventually fatally depth-charged by the Royal Navy, a British sailor clambered down a scrambling net, dangling over a ship's side, to rescue him from the sea.

§ HF/DF, or 'Huff-Duff', was an acronym for High-Frequency Direction-Finding, a technique invented in 1926 by a Scotsman, Robert Watt, who was a radio physicist and meteorologist. He had experimented with ways of tracking the radio signals that are given off by lightning bolts as the electricity in them ionizes the air. Watt realized that inventing a method of detecting the high-frequency signals from lightning would be a good way of tracking thunderstorms, and thus helping pilots avoid them.

‖ The U-boat record for surviving the largest number of depth-charge attacks was held by U-427, captained by the Austrian Carl Gabriel Graf von Gudenus. It never sank any Allied ships, none of its torpedoes ever hit their intended target, and its entire crew lived to see the end of the war, despite being depth-charged 678 times in one day.

Chapter Eleven

CLASSICAL ENEMIES0MODERN CODEBREAKING

At the start of World War II, Greece was governed by Ioannis Metaxas, whose political party called itself the 4th of August Regime, and who attempted to maintain a policy of neutrality. But the geography of Greece and its strategic position in the Mediterranean were to dictate otherwise. The turning point came at 8.25am on the morning of 15 August 1940. The Greek cruiser *Elli* was sitting at anchor just off the Greek island of Tinos, which lies in the Cyclades group in the Aegean. That week over southern England, the Battle of Britain was weaving vapour trails of agonized, vital confrontation in the sky. But in the turquoise waters off Tinos, and in the small towns on the island, it was a national holiday. 15 August is the feast of the Dormition of the Mother of God in the Eastern Orthodox Church – it celebrates her death and ascension into heaven. Some of the ship's officers and men were ashore but most were on board the ship when the Italian submarine *Delfino* fired three torpedoes at her. Nine men died as the cruiser sank. The same submarine then fired torpedoes at two Greek passenger ships sitting in Tinos' harbour. Shortly afterwards, fragments of the Italian torpedoes were recovered by Greek sponge divers from off the rocks of the island's harbour. With Italian markings on them, it was only too clear where they came from. Metaxas' government tried to pretend that the nationality of the submarine was unknown, but this did nothing to persuade the Greeks.

When Italian army units then moved to Albania, and established positions on the Greek border, war was certain.

In October 1940 Italian forces invaded Greece, with an offensive towards the area of Epirus, and the Greek–Italian war began. The Greek military, however, forced the Italians back over the mountains into Albania. The Italians counter-attacked in spring 1941, but were defeated again by the Greeks who were assisted by Albanian guerrillas, fiercely opposed to the presence of Italian troops in their country. The Greeks asked the Allies for help: Britain sent a handful of Hurricane fighters and some Blenheim bombers to assist in the war, and then, in March 1941, a full expeditionary force of British, Australian, New Zealand and some Indian troops. The Germans invaded Yugoslavia in April 1941, and then stormed into Bulgaria straight afterwards. The German tanks and half-tracks then pushed into Greece, their advance only slowed by fierce defensive actions by British and Commonwealth troops: at the Olympus and Servia passes, Australians and New Zealanders halted the 9th Panzer Division for three days. The attacking Germans and Italians had 1,350 tanks, the Greeks twenty, while their British and Commonwealth Allies had only 100. The German forces made swift progress, partly because almost the entire Greek army was still fighting in the Epirus area. Athens fell on 30 April and the remaining British units were taken off by boat to Crete.

Italy deployed both of its two codebreaking departments to war in Albania and Greece, and while the Italians concentrated on trying to break into Greek codes, the Germans were concentrating on trying to break into the Italians', and continuing with their efforts at breaking into the two field codes the British army was using. The war in Albania and Greece involved the Greek, British, German, Albanian and Italian armies, the Royal Navy, the Italian Regia Marina, the Kriegsmarine, and the U-boat service. Indeed the fighting in Greece in April 1941 was the overture to a wider, bigger naval and land war across the Mediterranean that would only really finish when the Allies took Italy back from the Germans, and the Greeks regained control of their own capital in 1944. The different navies, armies and air forces of the Germans, Italians and Allies clashed and criss-crossed in the scorching blue skies, on the cobalt seas of the Mediterranean, and in the mountains and olive groves of the Aegean, Peloponnese and Cyclades islands. Criss-crossing above and around them like so many electronic fireflies were the signals transmissions of all sides, the crackling whiplash of information in the ether

that was pulled from the sky, and read and monitored and translated and decoded by the cryptanalytic and signals intelligence agencies of all the different nationalities. The Mediterranean had seen fighting, combat and intrigue for 4,000 years: what made the war in 1941 so different was the technology used, the metal, the mines, the electronics and the aircraft. Every war brings new weapons, and new surprises that can help turn the course of events, and in this war, the new appearance on the stage came from the mysterious, misunderstood actor called cryptography.

•••

Shortly after the British forces clambered onto transport ships in Piraeus harbour in April 1941, a German Fieseler Storch reconnaissance aircraft flew high over the mountains and plains north-west of Athens. The pilot circled and climbed and returned to look down at the ground, as his restless passenger from the Luftwaffe scanned the landscape below for what he was looking for. The coastline was arid and dry in the August sun, rocks white and baked, valleys filled with juniper scrub and olive trees, a land of hovering buzzards, lizards and heat. Then the passenger signalled hard to the pilot, who flew around in a tight circle as they both looked below them at a flat plateau with a steep access road. Captain Ferdinand Feichtner, newly arrived from France, had found what he was looking for. A place to set up a perfect listening station that could cover the whole of the eastern Mediterranean. The location turned out to be the site of a former Greek Post Office installation above a small town called Loutsa, 160 miles north-west of Athens. The canny and hard-bitten Luftwaffe captain knew that his instincts had been correct. The dry and rocky hilly terrain was just a mile north of a transfer station for wireless traffic between Greece, Africa and London. Captain Feichtner, always one to be fighting against needless bureaucracy and incompetent senior officers, immediately decided to have twenty Rhombic aerials erected: these were wire direction-finding devices designed to intercept short-wave and high-frequency signals. He also drew up plans for an intercept building. A considerable battle was then necessary with the team of Luftwaffe construction engineers who had been sent in to help him, as they had their own pre-determined way of working, and the construction lasted a full nine months. Along with the construction of the building, Feichtner had to re-train the company who had come with him from France. This was vital

because the Luftwaffe captain knew that in the hot, clear desert of the Mediterranean and North Africa, signals intercept companies were going to be vital. Much of the war would be mobile, and land-based monitoring units would be able to intercept the enemy's signals from his armies, air forces and navies.

Meanwhile, the Italian army's intelligence agency Servizio Informazioni Militari, or SIM, had a cryptanalytic department that attacked foreign cryptosystems. This agency was headed by General Cesare Ame and was located in Rome. There were fifty people employed in its cryptanalytical section, half of whom were cryptanalysts, and the other half linguists and clerks. The Italian naval intelligence agency, on the other hand, was called the Servizio Informazioni Speciali della Regia Marina, or SIS, and was divided into four branches. B Branch was tasked with signals intelligence. It was sub-divided into cryptanalysis, interception and direction-finding, security and clandestine radio intercepts. The cryptanalytic department was located in Rome and was headed in 1940 by Admiral Luigi Donini. At the same time, while the Italians were decoding Greek naval messages, B-Dienst saw that the Greek communications could be used as a crib into the Royal Navy codes, as the British and the Greeks were sending signals to each other. B-Dienst's analysts took what the Greeks had written, and tried to cross-reference them with the daily messages sent by the British Royal Navy in the Mediterranean. This gave them a double-check system, as the Italians were by then sharing at least some of their naval intelligence with the Germans. The cipher system used for Greek air force communications was one of simple transposition.

Both the B-Dienst and OKW-Chi could see that the successive codebooks were based upon the 1935 Greek military codebook, and indeed before the Greek war started, back in 1939, Tranow had asked the Italian SIS and SIM if they could supply him with any breaks or 'cribs' they had into Greek codes. He assumed they would reciprocate partially, as they did. And then in 1941 he saw something which he had suspected, but had never yet had proof of. Information in Greek signals that indicated that the British were listening to Italian and possibly German radio traffic. A deciphered Italian signal ran as follows:

> *In addition, according to British liaison signals officers, Greek Signals Corps managed to decipher some Italian traffic during the November/December battles in Albania. On 6th December, a British lieutenant-colonel informed*

his superiors: 'Herewith a batch of Italian traffic intercepted by the Greek General Staff. Also, one copy of cipher "O.M." for internal use of the Italian Army in Albania.' On 8th December, the reply confirmed Greek success: 'Many thanks to Greeks for citrario O.M. Tell them I do not remember having seen it but I am very grateful for it and for any further documents of this nature which may be of assistance in reading Italian codes in Albania which I am afraid are not readable.' [1]

For the Germans, this was important. The information content of the actual signal in question was less important than the fact that they saw how they could develop another way of reading the signals of their allies and enemies, and also neutral countries. By reading a signal of one of their allies – Italy – they could also discover, by extension, what the British and Greeks did or didn't know about each other's codes, and about Axis signals intelligence. It meant that the Germans did not have to rely entirely on individual cryptanalytical successes – breaking the French war office code, for example – in order to be able to access information from other countries. By breaking one country's codes, such as Italy, they could then gain information about signals intelligence and cryptanalysis of third party countries.

By the spring of 1941 the signals intelligence agency of the German Heer was also solving Greek army and air force ciphers. Based by then in Belgrade, Bulgaria and later in Greece, it found that the Greek air force messages were a matter of simple boxes, with the text being sent in groups which had to be fitted into them. The 'indicator' took the form of three letters which were always in a given position, and so the first three letters of each group had to be removed before putting the cipher text into the given box. This was broken by writing out the cipher text in vertical strips of varying depth and sliding them against each other until a few Greek syllables appeared above one another.[2] After the initial break it became clear that a large part of the messages began with the words '*parakalao*', meaning 'please, I'm asking', '*anafero*' meaning 'I mention, or I report' and '*apesteilamen*' meaning 'I've sent it'. The width of the box was normally between fifteen and twenty-two columns wide, and the text had to fit into this box.

Back in Germany, OKW-Chi cryptanalyst Dr Walter Fricke was still meticulously keeping his diary, and making entries about the situation in the Mediterranean involving the Axis countries. The German diplomatic position with Mussolini, he said, was, on the surface, simple. The two countries were

allies, and allies did not read each other's messages. To keep records of technical information that proved that the reverse was the case contravened every German security regulation, but still Erich Hüttenhain's dutiful deputy kept his notes. He summed up the Italians and their early prowess with codebreaking thus:

> Mussolini had decided on war in the Balkans. Von Papen's warnings made Hitler averse to any immediate action there, but he was only able to restrain Mussolini to the extent of limiting Italy to war with Greece. In less than two months the Italians, who had the advantage in everything save morale, were badly beaten. The political leaders were terribly surprised and the Chief of General Staff, Marshal Badoglio, and numerous other high officers were relieved of their duties. This did not help matters.
>
> One of the most decisive factors during those weeks was the manner in which the Italians employed radio.
>
> The set-up was the same as that used in manoeuvres of previous years. They employed open circular traffic; that is, they used one uniform frequency for a group of stations belonging to the same unit (e.g., the stations of three infantry regiments of a division for traffic with one another and with the divisional station) and each station used only one call-sign for all its traffic. The call sign was supposed to change daily but was often used for several days; not infrequently a change in call sign was followed by errors which betrayed the change. Traffic was so heavy that the enemy always had a chance to take bearings and fix locations. Frequently messages were sent in clear. Several units of the Italian Eleventh Army distinguished themselves in this respect. Moreover, the Greeks had obtained at least two Italian army cryptographic systems, how I do not know, but it is certain that in the very first days of the campaign they could decipher a large part of the Italian messages. This enabled them to learn promptly most of the dispositions of the Italian command and to take appropriate action. The superiority thus gained was utilized cleverly and a series of military actions took place which heretofore would never have been deemed possible.[3]

It was a stellar use of codebreaking and signals intelligence, but it did not stop Greece from losing the confrontation with Italy. But then the Italians did

something that surprised everybody in its audacity, a cryptographic operation whose strategic and tactical results almost changed the course of the war in North Africa, and nearly enabled Rommel to reach the Suez Canal.

PART THREE

GERMANY AT WAR

Chapter Twelve

GERMANY'S MEDITERRANEAN BATTLES

1941–1942

By the spring of 1941, both the Germans and the Allies were listening to each other. The Allies had begun to read signals encrypted by the Germans on their naval Enigma machines, using the encryption cipher that the Germans codenamed 'Triton', and that the British generically called 'Shark'. The Luftwaffe were using a four-rotor Enigma to encode their signals to fighter and bomber squadrons in France, Italy, Yugoslavia and Greece. Despite three repeated requests from Luftwaffe signals intelligence, and early suspicions that the British could even be reading it, they had not changed its settings. The Royal Navy were putting this information to good use. They had sunk three Italian heavy cruisers at the Battle of Cape Matapan in March, having ascertained their positions off the Peloponnese Islands via Enigma intercepts. Then a Royal Navy boarding party from the destroyer HMS *Bulldog* captured the German submarine U-110 in May during a convoy battle in the Atlantic, and rescued its Enigma machine and codebooks, enabling the British to reduce their decryption time of some Enigma intercepts from eleven days to five hours. But even following these events, both the B-Dienst and the Luftwaffe refused to entertain the possibility that the British were making inroads into reading their codes.

After the Battle of Cape Matapan, Admiral Andrew Cunningham told his

subordinates that the battleship *Vittorio Veneto*, and the cruisers *Zara*, *Pola* and *Fiume* had been found by a Catalina seaplane from Crete. The information was almost certainly broadcast back to the Admiralty in London in the naval code the Germans now called 'Munich'. In Neumünster, the B-Dienst monitoring station would have intercepted the first three five-letter code groups of the message, read the Morse code, and sent them by teleprinter back to Flensburg. Tranow and the Germans believed the story about the Catalina, but to cover the B-Dienst's inroads into 'Munich', they let it be known that failures in Italian intelligence were also to blame, and that they had an informer in the ranks of the Italian naval staff who had somehow let slip the information about the movements of the Italian naval vessels.

Despite the fact that both sides were now making mutually camouflaged advances into each other's codes, when accurate and timely signals intelligence went hand in hand with the tactical and strategic means to use it properly, disaster could still strike. It nearly did so in Crete. Despite an equivalence and parity in their respective levels of signals intelligence, both sides then failed to maximize its potential to their own ends. From breaking Enigma, the British knew some of the German plans for the invasion a month in advance, in March 1941.* They were reading both the Luftwaffe's Enigma and parts of 'Shark', and followed in detail the build-up of German troop-carrying vessels, Junkers Ju 52 transports, escort destroyers and embarkation procedures for Luftwaffe flak units. Everything about the German plans suggested that Crete was going to be the target, but the British were convinced that it was a deception operation which was designed to camouflage a German attack on Cyprus or Syria. Three weeks before the invasion, it became obvious that the Greek island was the real intended target of the Germans, and this gave the Allies time to build up their defences. Australian, British and New Zealand troops were ferried to ports on both the north and south of the island. The RAF tried to reinforce their meagre presence on Crete; but of the aircraft they sent, few were operational. The Germans had complete air superiority: some 1,200 aircraft of all types were deployed in the invasion of Crete. The RAF had four squadrons on Crete, totalling some sixty aircraft, but because of lack of spares and support only some twelve actually worked.

But if the British preparations on Crete were lacklustre in the extreme, then so was the German intelligence response. Each branch of their signals

intelligence apparatus seemed to be giving different information. The Abwehr covered up their lack of clear information from agents in Cairo, Athens and Turkey by blaming the B-Dienst and OKW-Chi for not providing enough signals intercepts. They said that the Luftwaffe's new signals monitoring station north-west of Athens, run by one Captain Feichtner, should have picked up more Allied transmissions. They duly reported the information right up the chain of command to Hitler and his chief of staff Field Marshal Keitel that, at most, there were 5,000 British troops on the island, and that the Cretans were predominantly disposed to support the Germans. The reverse was, of course, the case. There were very roughly 48,000 British, Commonwealth and Greek troops on the island, and the predisposition towards the Germans of the majority of Cretans, as well as of Greeks evacuated from the mainland, was one of open hostility. Crete was a perfect example of a battle where both sides had relatively clear and true information about the enemies' intentions, gained from good signals intelligence, but both protagonists then proceeded to squander this, and then to waste their tactical advantage so gained.

But out of the debacle of Crete, the B-Dienst profited. On 26 March, the British heavy cruiser HMS *York* had been hit in Souda Bay by two Italian explosive motorboats of the Italian navy, launched from destroyers. Two old Italian warships were fitted with special cranes to operate these assault craft, and six motorboats entered the bay, and attacked three targets in pairs. The first was HMS *York*, the second was the tanker *Pericles* and the last was another ship at anchor. Three of the attacking boats had various problems, either mechanical or human, due to the extreme temperature conditions, but the other three successfully attacked their targets. Two of the motorboats, packed with 730 pounds of explosives in their bows, struck *York* amidships, flooding both boiler rooms and one engine room. Two British sailors were killed. All the Italian sailors survived the attack and were captured by the British, and the cruiser was run aground to prevent it from sinking. A submarine was then used to supply electrical power to operate the cruiser's guns for anti-aircraft defence, until it too was severely damaged by air attack and had to be towed away for repairs. When the Italian motorboats had been sighted, *York*'s captain had taken three copies of the Royal Navy Cypher No. 2, his subtractor tables and slides, and carefully poured a glass bottle of sulphuric acid over the codebooks. He then jumped over the side and was rescued by a lifeboat. A week after the start of the German invasion of 20

May, two divers from the Kriegsmarine entered the wreck of HMS *York*, and in the captain's cabin they found the codebooks. The acid had been only partially effective. The codebooks were flown to Athens and then to Berlin. One of Wilhelm Tranow's staff estimated that at least 50 per cent of the cipher groups could be reconstructed.

However, the successes of the B-Dienst with the decryption of the codebooks captured from HMS *York* were nothing in comparison to one of the signals intelligence coups about to be carried out by the Abwehr, OKW-Chi and the codebreakers and monitors of army headquarters.

As far back as 1935, when Mussolini had taken Italy to war in Abyssinia, the Third Reich had been taking advantage of the Italian signals intelligence and cryptographic apparatus for its own ends. Wilhelm Tranow and the early personnel at the B-Dienst had used the radio signals of Italian naval ships as cribs with which to break into parts of the codes used by the Royal Navy ships in the Mediterranean and the Red Sea. Knowing part of the Italian naval codes, the names of their ships and their positions, he had enough information to begin to break into the messages the British transmitted, when they in turn were reporting the Italian daily positions back to the Admiralty in London. The Italian SIM had a member of staff who worked at the Vatican, the Holy See, in Rome. In summer 1935, the SIM persuaded one of the Italian staff who worked at the British diplomatic mission in the Vatican to photograph the British signals codebooks.

By the beginning of 1941, the regular army's signals intelligence and cryptographic unit was still formalizing its existence and administrative structure after the ad hoc duplication of effort that had accompanied the invasion of western Europe. The OKH-GdNA, as noted previously, was the abbreviation for Oberkommando des Heeres/General der Nachrichtenaufklärung, and was the signals intelligence agency of the German regular army, the Heer, before and during World War II. It had taken over some of the military responsibilities from the OKW-Chi in 1939. At first, however, between 1940 and 1942, the unit had not yet assumed its full lengthy title, and so was called Inspectorate 7/VI of the OKH. This was shortened to In 7/VI.

Each regiment of the regular army, which varied from 800 to some 1,100 men, would have a signals company attached to it, which would include a monitoring and intercept platoon. A brigade, the parent unit of a number of regiments or battalions, would include an entire intercept company all of its

own. Six new signals intelligence regiments were the mainstay of the monitoring, intercept and decryption capacity of the Heer. They were each called Kommandeur der Nachrichtenaufklärung, or KONA for short. Each one was attached to an army group: 1, 2 and 3 were assigned to the Eastern Front, 4 was in the Balkans, 5 was on the Western Front in France, and 6 was a roving unit that covered the Mediterranean with its various units split up across the theatre. Each long-range signals intercept company in each KONA was called a FAK, an abbreviation of Nachrichten-Fernaufklärungs-Kompanie.

In March of 1941, one such company arrived in North Africa. It had crossed the Mediterranean in a supply convoy, at repeated risk of attack from Allied submarines and aircraft. The company's commanding officer, Captain Alfred Seebohm, did not arrive until 24 April, when he brought another radio intercept platoon, a radio direction-finding platoon, and a group of cipher specialists. They were posted to Sirte in Libya, half-way between Tripoli and Benghazi, and there were around 300 men in the unit, which was called the 3rd Company of the 56th Signals Battalion. Only later did the unit become known as FAK 621, or 621 Company, the nomenclature under which it would achieve notoriety on both sides of the front line.

The men in the unit had operated in Greece, on Crete, in France and in Norway. They had been selected from their previous units for their different skills, and they were broken down into four different groups. There were the signals intercept operators, whose job it was to sit in intercept trucks, and scan a variety of radio frequencies. Once they had picked up the Morse code transmission of, say, a company of the British Rifle Brigade, they noted down the initial code groups which resulted from transcribing the Morse into plain English text. If the signals operators working with the British light infantrymen were dispatching a report to their battalion headquarters about a successful patrol the previous night, which had resulted in the capture of three German prisoners, the message would be prefaced to the code of the battalion headquarters, encrypted in the code which the Eighth Army were using. At one time the call-sign of the Eighth Army was 'MXQ' so a company or battalion or brigade message would be prefaced by these letters. It would normally be led into and finalized with strips of super-encipherment, so the messages the Germans would hear in Morse would consist of strings of five- and four-letter groups with the actual message concealed within it.

If the 3rd Battalion of the British Rifle Brigade's unit call-sign that month

was GBB, their parent brigade SDQ, and the Eighth Army MXQ, the letters GBBSDQMXQ would occur in the lead-in to the message, interspersed with strips of encipherment. So if the code being used was a four-letter one, then the initial lead-in to the coded message would read GFTTU*GBB*OIYCM*SDQ*MQAE*MXQ*, where the initialled letters were parts of the message, the five-letter groups the camouflage of encipherment.

Knowing from previous messages that the British would be using a four-letter code, the German signals intercept operators would listen for fourteen-letter bursts of Morse code, and transcribe these. Once they had a string of letters sitting on the signals pad in front of them – sand, sweat, dust and flies also jostling for space on it – they passed it to the language monitors with whom they worked side by side in their trucks or tents. These men saw that they had groups of letters which represented a message in English, so they would initially look for letter groups they had identified from previous messages, and letter groups where commonly used letters in the English language – E, T, A – repeated themselves under the guise of coded letters. While they worked on trying to identify letter groups, they would send the intercepted messages upwards to their regimental headquarters, who would in turn pass it back to the In 7/VI by teleprinter. The message would thus be worked on simultaneously by two parties. Because the army in North Africa was far flung from Germany itself, or its main strategic out stations like France or south-eastern Europe, the Heer attached groups of cryptographers and linguists to field units. The third group of men in the signals intercepts companies consisted of those whose job it was to erect, maintain and position the direction-finding aerials which physically picked up the electronic radio impulses. The fourth acted as regular infantrymen, guarded the others and maintained the vehicles.

On the one hand, North Africa was a perfect working environment for a signals intercept operator. The air was warm and comparatively clear, except in the case of sandstorms, and there were very few physical obstacles like forests or mountains or cities. Radio signals tended to travel without interruption as they had fewer obstacles to bounce off, as with Ferdinand Feichtner's Luftwaffe intercept unit based south-west of Athens, set on a mountain plateau. The Western Desert was similar to the sea in many ways: finding the enemy was part of the operational imperative. The huge terrain involved meant that warfare was mobile and fluid, and each unit had to keep in touch by radio. But North Africa had its harsh disadvantages. Many of

Captain Seebohm's men had not travelled outside of Europe before the war. The men from Bavaria and Saxony and the Rhineland had never known such heat, nor, at night, such abrupt drops in temperature. During the day, the enemies were the sun, sand flies, dust and dirt; few soldiers had access to, or used, any form of suntan cream. A German company that before the war had produced sun-cream for skiers had issued its product in limited amounts to limited units, but for most of the German soldiers, sunburned necks, faces and arms were the order of the day. Water was strictly rationed, and the soldiers had to wash and shave with it as well, while the omnipresent sand led to rashes and skin infections. Mild gastroenteritis and diarrhoea were the result of drinking dirty, often salted water. Sometimes many men found that the sandy dirt that seemed to cover them day and night provided the best protection from the glaring sun. Despite these conditions, they excelled at signals interception.

The mobile nature of the warfare provided its own paradoxical problems. The unit had to be on the move to follow the ever-moving front line, but it was impossible to work and intercept signals on the move. So for the officers, the main priority was to find a position that was firstly, near the front line, secondly, relatively safe, and thirdly, positioned so that the radio intercept aerials could 'grab' traffic. The operators worked primarily on the high-frequency radio bands, and one way to intercept signals was to listen out for conversations or communications in open speech, which parts of the Eighth Army transmitted frequently. Apart from trying to find out what the enemy was doing, the German signals officers were attempting to discover who the enemy was, and thus build up an Orbat, or Order of Battle of the units ranged in front of them. The British set up their radio networks in much the same way as the Germans, with a control station and a number of out stations. All traffic was centrally steered through 'control' and back again, in a pyramid formation that bounced backwards and forwards. Each station had a call-sign, and as the intercept operators found the various British radio nets, they had to determine what radio network they were listening to and its purpose. The British made their job much easier in mid-1941 through lax communications security, as they did not always use code words. A British radio operator might try to contact Eighth Army instead of MXQ. This meant the Germans knew what MXQ was, and the British compounded the problem by not changing the various code words very often.

Several other factors enabled Seebohm's men to build up a picture of the

unit in front of them. The first was the individual British Morse operator's 'fist' which was unique to each man. Because the British often failed to switch their different radio operators between different units, it was thus possible to identify each unit's radio signaller. The call-sign of a unit might change, but the signature indicator of the operator's Morse didn't. The Germans were rigorous and disciplined and patient, as well. Everything they heard was passed upwards or backwards for evaluation, and within a matter of days in a certain position the company started to build up a picture of which unit was operating in front of them. On the rare occasions that they actually captured enemy codebooks, this obviously enabled them to read into the British codes, but also helped to build up a detailed tactical picture of the enemy soldiers and armour operating in front of them. Every day Seebohm created a radio situation report from the various inputs of the company, and to make sure that his signals kept pace with General Erwin Rommel's constant movements, he attached a small liaison unit of his men to general headquarters. In mid-May, Seebohm's first success occurred when his men noticed that all the British units facing them suddenly, within forty-eight hours, included the same code word in every one of their radio messages. His company deduced that an offensive was likely: then their direction-finding platoon detected a sudden large movement of British armoured units near Sollum, and on the evening of 14 June 1941 one of Seebohm's keen-eared signal interceptors heard the one-word code used again. Seebohm informed Rommel that a British offensive was almost certainly imminent and Rommel immediately shifted his forces.

The British offensive, codenamed *Battleaxe*, began the next day. It was an attempt to drive German and Italian forces out of Cyrenaica and to try to push through to relieve the beleaguered garrison at Tobruk. The German unit intercepted a lot of significant traffic in the clear during the battle, where British commanders debated the movements of different units, and also reportedly complained about the lack of ammunition, but early in the battle the Germans also captured a British codebook. Immediately, however, the British suddenly imposed radio silence, which allowed the British 7th Armoured Division – heavily outgunned – to withdraw without the Germans noticing; the 11th Hussars and the 4th South African Armoured Car Regiment then changed their radio operators, so the German signals intelligence units were now unsure as to which unit they were listening to. The operation was a failure for the British, and then subsequently Captain

Seebohm and the entire signals and intelligence-gathering infrastructure of Rommel's army had a break bigger than anything they had ever anticipated.

---

* The British operations to read German signals encrypted with Enigma are described in subsequent chapters.

Chapter Thirteen

LOSING ENIGMA

From the Mediterranean to the Western Atlantic, from Bear Island in the northern Arctic to the Falkland Islands in the south, and from Cadiz to Moscow, Allied and German cryptanalysts and signals intelligence staff were now trying to listen to each other's signals, and attempting to decrypt them. Both sides, naturally, knew that the other was trying, but in general neither side knew the exact extent to which the other was, or wasn't succeeding. It was similar to a game of chess where neither player can see the other pieces, or the far side of the board, while the game was being played three-dimensionally. If the Germans had been reading the British Royal Navy's codes, and the British in turn were reading the German Kriegsmarine's Enigma-coded signals, and both sides were reading parts of Italian codes, while the Italians in turn were reading some of the British navy's encrypted messages, then were all sides able to reverse the encryption breaks and read back into each other's messages? And if the Germans had cracked the French military cipher, parts of the Romanian and British diplomatic codes, and the Swiss Enigma, then did it follow that the British could therefore piggy-back onto these breaks themselves? Nowhere was the game of chess so bitterly fought out, on such an operationally vital battlefield, as in the northern Atlantic. While Wilhelm Tranow, Erich Hüttenhain and Ferdinand Voegele had been trying to decode their enemy's signals, what had the British been doing in turn, and were the Germans in any way aware of this? And if so,

what were they doing?

The Government Code and Cypher School at Bletchley Park

In 1938, Bletchley Park was a small country house, sitting near Bletchley railway station about fifty miles north-west of London. In 1883 the house's estate of 581 acres had been based around a large farmhouse, but the new owner, a Liberal Party politician called Sir Herbert Samuel Leon, had expanded this building into what one architect called a 'maudlin and monstrous pile' that combined the different styles of Victorian Gothic, Tudor and Dutch Baroque. In 1938, Admiral Sir Hugh Sinclair bought the mansion and fifty-eight acres of surrounding land for £6,000. He was a former director of naval intelligence, and had become head of the Secret Intelligence Service, also known as SIS or MI6. An SIS story, which has become legend, says that Sinclair used his own money for the purchase, as the government claimed they did not have the budget. His aim was to use it as a signals intelligence base in case of war. Bletchley Park was centrally located, on the junction of two main railway lines, and a main north– south road, and there was also a telegraph and telephone repeater station in nearby Fenny Stratford. Sinclair was prescient and far-seeing about the impending threat from Germany. In December 1938, he prepared a dossier on Adolf Hitler for the British prime minister and the foreign secretary. Sadly, he was to die of cancer that same year, before war broke out.

He wrote of the German leader that he possessed:

> … fanaticism, mysticism, ruthlessness, cunning, vanity, moods of exaltation and depression, fits of bitter and self-righteous resentment, and what can only be termed a streak of madness; but with it all there is a great tenacity of purpose, which has often been combined with extraordinary clarity of vision. He has gained the reputation of being always able to choose the right moment and right method for 'getting away with it'. In the eyes of his disciples, and increasingly in his own, 'the Führer is always right'. He has unbounded self-confidence, which has grown in proportion to the strength of the machine he has created; but it is a self-confidence which has latterly been tempered less than hitherto with patience and restraint.[1]

Commander Alastair Denniston, who had worked at Room 40 during World War I, was the operational head of the Government Code and Cypher School from 1919 to 1942, and he moved the department's cryptanalysts to Bletchley from London just after war was declared. Already, the British had done something the German signals intelligence empire had not: imposed a centrality of location and collectivity of effort. The recruits to 'the Park', or 'BP' as it was known to those who worked there, were in many ways similar to the German cryptanalysts. Mathematicians, chess players, linguists, those who excelled at cryptic crossword puzzles. Cambridge and Oxford universities provided many recruits, some described by Denniston as being like professors. Unlike the Germans, women were recruited in large numbers for administration and clerical jobs, many from the WRENS, the Women's Royal Naval Service. In 1941, the *Daily Telegraph* newspaper was asked to organize a crossword competition: contestants who had done well were subsequently approached to see if they were interested in contributing in a particular way to the war effort.

Like the Germans, Bletchley relied on a network of listening stations. These were set in Norfolk, Leicestershire and Bedfordshire; the coded intercepted messages were taken down by hand, and the messages sent to the Park at first by motorbike courier, and later by teleprinter. The Code and Cypher School's decryption and cryptanalytical capacity also differed hugely from the Germans', in as much as it was all carried out in a series of wooden huts and outbuildings in the grounds of the same building. Keeping all of the country's major codebreakers together meant it was much easier to ensure a collective atmosphere of security and confidentiality. The output of Bletchley Park was classified as above Top Secret, as 'Ultra-Secret'. From here sprang the words Ultra Decrypts that were commonly used by the Allied intelligence establishment for the decryption efforts and resulting intelligence that the Cypher School produced. Each 'hut' was akin to an individual department. One hut handled German army and air force decrypts, another analysis of naval Enigma, another Italian, Spanish and Portuguese decrypts, while others handled Wehrmacht and Luftwaffe Enigma, plus coded messages sent by the Abwehr, while one whole building housed the 'bombe' machines used to mass-process Enigma coding permutations.

A Game of Chess

At the meeting in the woods at Pyry south of Warsaw in July 1939, the Poles had given the French and the British what they knew of the workings of Enigma. After the invasion of Poland and then the fall of France, some of the Polish mathematicians and cryptanalysts who had escaped based themselves at Cadix in the unoccupied zone of France, supplying limited amounts of intelligence to the British. At Bletchley, the fundamental achievement was made by Alan Turing and his team, who modified the Polish 'bombe' mechanism to provide a form of computerized cryptanalysis. The basis of this required imagining what the original plain text of a German message might be for a particular day. The bombes, which were essentially a huge collection of Enigmas, would then spin through every single possible rotor combination to see if the result could yield the cipher text from the assumed plain text. If the bombes did their work, then the rotor combination that they gave up represented the day's Enigma key settings for that particular network of keys.

There were a variety of ways the British made informed guesses at the plain text, which was what the Germans were trying to keep secret. Sometimes the Germans sent identical messages in two completely different cryptosystems; one would be dispatched to an infantry company who didn't have an Enigma machine, or who had lost it. So if a unit had not been issued a machine, had lost it, or had damaged it, they would receive a message that was obviously not encrypted on Enigma. A unit that was equipped with the encryption device would receive it in one of the Enigma codes. A message text thus existed that was both encrypted and in clear, coming from the same source. The first would provide the crib into the second. German commanders in the field would occasionally send the same plain text message at the same time each day: '*Nothing to Report*', '*Front Line Calm*', '*Daily Summary*', '*Ammunition Status*'. This approach worked most often with the Luftwaffe, whose pilots, ground crew and aircrew were considerably less respectful of radio discipline than the army. The most disciplined radio operators were the Kriegsmarine, and of these, the U-boat service excelled. However, despite their reputation for radio discipline, the U-boats were required to send a large volume of messages each day that were often identical in content: weather reports, location and convoy sightings. But far more often, Bletchley Park could only guess at the content of the German plain text, unless they had one of a series of crib words. If a U-boat sent three location reports in one day during which the day's Enigma key setting remained unchanged, at least five of the letters of the message – the U-boat's individual identification sign –

would be the same. If no such crib existed, then Bletchley Park's cryptanalysts were reduced to guesswork, and using the bombe machines to spin through millions of possible permutations.

Another way of trying to arrive at the plain text was through capturing Enigma codebooks, rotors, signal books, or, the most prized, an entire operational Enigma machine. The British Royal Navy quickly devised several different plans on how to do this. Their first success, mainly through luck, came on 12 February 1940.

U-33 was sailing outside the Firth of Clyde, off the west coast of Scotland, on a mission to sow mines. The minesweeper HMS *Gleaner* depth-charged her, forcing the submarine to the surface. Before the crew left the conning tower of the submarine, some parts of the Enigma machine, including the rotors, were distributed among the members of the crew so they could throw them into the sea as soon as they left the hull of the boat. One of the German sailors forgot to throw his requisite parts into the sea, and when he was picked up by the British sailors, they found three rotors in the pocket of his trousers. Up to eight different rotors were then in use in different Enigma machines, numbered I to VIII. Three of them, VI, VII and VIII were only used by the Kriegsmarine. In the pocket of the German sailor, they found three rotors, including VI and VII. The British didn't know the wiring configurations of these two rotors, so this was an unexpected surprise. However, until they could find Rotor VIII, they were still a long way distant from breaking into German naval Enigma with any degree of regularity.

From 1939 onwards, as the German and British chess players sat opposite each other, a list of some of their opponents' pieces that they had taken from the board looked like this. The Germans had started reading the British Royal Navy's Administrative Code, Naval Cypher No. 1 and the Interdepartmental Cypher before war broke out. In 1940 they added the British Merchant Ships Code, and the Submarine Code. The British had broken into the German Merchant Navy cipher in September 1939, and the Luftwaffe Enigma codings in October of the same year. By March of 1940, the first purpose-built bombe at Bletchley was starting to help them solve Enigma-encrypted messages faster. Neither side, at this point, suspected or knew that the other had or was decrypting any of their messages. The British assumed that if the Germans had made any breaks into their codebooks this could be rectified by either changing or replacing them. As for the Germans, not only did they not suspect that the Allies had started making inroads into Enigma, they thought

it impossible.

The Royal Navy's Cypher No. 1 had remained unchanged since 1934, and the Germans had reconstructed and were reading it until finally, after six years, the British Admiralty replaced it with the Naval Cypher No. 2. Again, this was based on a codebook, which worked in combination with a subtractor enciphering table. At the same time, the British introduced the General Recyphering Tables, which were a book of uniform, four-figure subtractor tables that were to be used with all the British maritime codes from then on. After seven weeks of work on Naval Cypher No. 2, Tranow and his men discovered the meanings of 800 code groups, 400 words of general vocabulary and 450 ships' names. This was a huge advance and meant that he could identify the location of several battleship and cruiser flotillas, and also nearly 300 merchant ships. As these now sailed in convoys across the Atlantic, it was thus a straightforward process to identify which convoy they might be sailing in, from where, when and whether bound westwards to America or eastwards to Great Britain. From October 1940, the British Admiralty introduced a reciphering procedure based on Left and Right Subtraction, and then two additional reciphering tables, one for use in the North Sea and Atlantic, the other in the Mediterranean. By the start of 1941, Tranow had expanded the list of code words he had decrypted to 700 ships' names and 1,200 words of vocabulary. He started to assign British codes with nicknames, based on German cities. The Naval Cypher was 'Cologne', and the Naval Code was called 'Munich' with two variants, 'Brown' and 'Blue'. On 20 January 1940, the Admiralty introduced disguised starting-point indicators. This meant that the indicators, instead of coming at the beginning of the message, were hidden in the text at a pre-arranged point. It took the B-Dienst a month to start reading into it again, but once again, a shortage of staff left Tranow hamstrung, and after a month he could only read some 10 per cent of the messages.

The chess game continued; in January 1941 Bletchley Park broke the Luftwaffe key for North Africa, and in March the Royal Navy's victory in March 1941 at the Battle of Cape Matapan was assisted by breaks into Italian naval Enigma which told Admiral Andrew Browne Cunningham – nicknamed 'ABC' – the locations of Italian heavy cruisers. Tranow struggled to keep up: he seemed to be fighting a losing battle to keep hold of trained staff, and to recruit new ones. By the time of Cape Matapan, sixty-four men were assigned to decrypting the British Naval Cypher, on four watches of six

hours each. He needed another twelve men at least – forty people alone worked on one separate sub-division for the Royal Navy's codes. During the whole period of the war, B-Dienst suffered from a chronic shortage of personnel. In April 1941, a total of sixty-four personnel had been assigned to the decryption of the principal Royal Navy Code, working shifts of six hours each, and Tranow estimated that to make the advances he needed into these British naval codes he would require another 165 staff for this task alone. This problem with recruitment was not something, by comparison, that hindered Bletchley Park at all. When four of the heads of section complained to Winston Churchill in 1941 that they had a shortage of personnel, he sent one of his notorious messages headlined 'Action This Day' to his staff, ordering them to provide the Government Codes and Cypher School with whatever they wanted.

On 1 February 1941 the Kriegsmarine had added a fourth rotor to their standard Enigma machine, and although the new rotor did not turn automatically alongside the others, it could be set to one of twenty-six positions. One of these, called Position A, converted the machine to a standard three-rotor, allowing it to send or receive messages either in the standard mode, or in a special Kriegsmarine-only mode. Transmissions sent under the latter were by now known by the British as 'Shark'. The British knew that to be able to make any form of advances into the German naval codes, they had to find a way to capture, if not an Enigma machine with its rotors intact, then at least one or more of the codebooks that U-boats and naval vessels used.

One of Bletchley's cryptanalysts suggested that a way to do this would be to target German weather ships; these were trawlers and converted frigates that the Germans deployed in the North Atlantic to gather meteorological information about cloud cover, thunderstorms, pressure fronts and other details that could affect their naval operations. What if, said Bletchley, we were to try to board or sink or capture a weather ship? When these vessels sent a meteorological message, it was condensed into a few letters with the help of their Short Weather Code; these letters were then enciphered with Enigma, deciphered by German colleagues at the B-Dienst's meteorological section, and then broadcast back out to warships and submarines. Because the weather codes always contained the same words and information – the ship's position and name, barometric pressure, cloud cover – they made excellent cribs for Bletchley Park.

The British made a start on 4 March 1941 when commandos raided the Lofoten Islands, off the north of Norway. A Royal Navy destroyer, HMS *Somali*, damaged a German fishing trawler, the *Krebs*, and British sailors boarded it. In the captain's cabin, one of them found a wooden box containing two Enigma rotor wheels, the key tables for February and the plugboard setting. The German captain, Lieutenant Hans Kupfinger, threw his Enigma machine overboard. Spring 1941 continued to be a successful season for Bletchley Park. On 9 May, U-110 attacked a westbound convoy near Iceland. The captain of the submarine was Fritz-Julius Lemp, who had torpedoed the British passenger liner SS *Athenia* in 1939. He torpedoed two freighters but in turn was depth-charged by an escort ship, which forced the submarine to the surface. The destroyer HMS *Bulldog* set to ram her, but its captain then realized that he might be able to capture the submarine intact, so the British boarded her. The radioman had made no efforts to destroy the Enigma or throw the keys overboard, so the Royal Navy boarding party recovered the submarine's naval Enigma with its rotors and the key settings for June. Lemp drowned swimming back to his submarine when he realized that scuttling charges were not going to explode – although a German version of events claimed that British sailors shot him in the water. The Germans did not realize that the submarine had been captured, or that they had lost the Enigma machine, and Rear Admiral Dönitz received a report that said the U-boat had disappeared with all hands. When the first set of Enigma keys arrived at Bletchley Park on 1 June, the solution time for a message encrypted that month on a German naval Enigma fell from eleven days to five hours.

The captured information bore direct results, one of which was the sinking of a German commerce raider, the *Atlantis*. In 1940 and 1941, it sank or captured twenty-two Allied ships totalling 140,000 tons. One of these was the SS *Automedon*, which was a passenger and cargo ship attacked by the *Atlantis* on 11 November 1940. At 7am that day, *Atlantis* sighted the *Automedon* 250 miles north-west of Sumatra, and at 8.20am *Atlantis* raised a German naval ensign and uncovered the guns hidden on its deck and in the sides of its hull. *Automedon* immediately began transmitting the signal 'RRR', meaning it was under attack by a surface raider. *Atlantis* opened fire from 2,000 metres, hitting the *Automedon* and stopping it dead in the water. A German boarding party found not just confidential operational mail on its way to the British Far East Command, but several decoding tables. Then on 11 July 1941, the *Atlantis* opened fire on the passenger liner *City of Baghdad*,

and another boarding party discovered a copy of the codebook titled *Broadcasting for Allied Merchant Ships*, which contained communications codes. On 18 October, the captain of the *Atlantis* was given orders to make a rendezvous with the submarine U-68 south of St Helena, refuel her, and then head north to Ascension Island to refuel another submarine, the U-126. The signal from German Naval High Command, the OKM, was sent encrypted in the naval Enigma cipher, and Bletchley Park intercepted it and read it. The British cruiser HMS *Devonshire* was sent to attack *Atlantis*, and on the 22nd it did just that. The Germans had gained the British merchant shipping code, but had lost the highly successful *Atlantis* because they had lost, and were continuing to lose, the secrets of Enigma. Rear Admiral Dönitz was still none the wiser.

By late 1941, on the German side of the chess board that was the cat-and-mouse chase of mutual naval codebreaking, one of the B-Dienst's biggest successes was the breaking of the British Combined Naval Cypher No. 3, which the Admiralty had newly introduced on 20 January 1941. The codebook, a four-figure encryption enciphered on a subtractor table, was designed for both the British and Americans to communicate with Atlantic convoys. Tranow and his men called it the 'Convoy Cypher' for short, and codenamed it 'Frankfurt'. The subtractor tables used with Naval Cypher No. 3 had 15,000 groups in 1941, and as the signals traffic increased in the Battle of the Atlantic, so did the size of the subtractor tables, containing over 200,000 letter groups by mid-1942. The Allies' mistake was that they re-used code groups several times, meaning that the Germans then had depths from which to reconstruct the cipher.

To add to their success with 'Frankfurt', the Germans further back-footed the British at the beginning of 1942 by introducing a new version of the Short Weather Code, meaning that the cribs the British had taken from the *Krebs* and the U-110 were no longer of any use. The Germans did not stop there; intensely concerned that the Allies must be trying to break into their cryptosystems as well, especially given the hugely increased volume of signals being transmitted during the Battle of the Atlantic, they changed the configuration of their naval Enigma, and in February 1942 added a fourth rotor to the original three. This one was not simply a rotor that allowed the naval Enigma to switch at will between standard three-rotor settings, and the Kriegsmarine setting, but a fully integrated rotor system that multipled by twenty-six the already existing permutations of settings. The Allies were now

blind to 'Shark'. Sinkings of merchant vessels from June to December 1942 were consequently quadruple those from the same period a year earlier. It was estimated that through reading Enigma, and the subsequent production of Ultra material, the Allies had reduced their losses at sea by 65 per cent by the second half of 1941, but this situation was now reversed.[2]

And by April of that year, the Germans reconstructed and could read the entirety of the British and Allied Merchant Ships Code helped by the codebooks captured by the *Atlantis*. Tranow and his teams had reconstructed this with impressive speed, helped by an influx of new staff. By early spring 1942, the B-Dienst was thus able to read, almost daily, the Admiralty U-boat disposition signal, often on the same night it was produced.[3] Using this information, B-Dienst could forecast the routes that convoys would take to avoid concentrations of U-boats referred to in the signal, and take appropriate action. On the chess board, the Germans had just taken the Allies' queen.

Chapter Fourteen

THE GOOD COLONEL

Three months before the United States joined the war, their embassy in Rome was still neutral territory, but in September 1941, the head of Italy's military intelligence service decided to burgle it. General Cesare Ame was in charge of the SIM. Italy was fighting against the British in North Africa and the Mediterranean, and losing, and although it was allied with the Third Reich, they had a mutually distrustful relationship. Ferdinand Feichtner of the Luftwaffe was to say he would not trust the Italians and would prefer not to share intelligence with them. The cryptanalysts in Rome therefore needed an intelligence lead. So Ame approved a break-in of the United States embassy in Rome. His target? Their diplomatic and military codebooks. The actual operation to burgle the building turned out to be the most straightforward part of the operation: since Ame had keys to all the embassies in Rome, except for the Russian one, it was a simple matter to gain entry at night. He went to choose his team. There were four of them: two national Carabinieri police officers, and two Italians employed by the embassy. One of the latter, a messenger called Loris Gherardi, was chosen to open the safe in the military attaché's office.

The four men waited until nightfall, and until all of the American diplomatic staff had long gone home, so it was after midnight when they approached the large, pillared building on the city's Via Veneto. The orange trees and palms on the sloping boulevard outside the gates gave them some of

the shadow they needed. They opened the main entrance gates – which Gherardi had left unlocked earlier – and walked quickly across the still-warm flagstones to the main entrance. Four minutes later, they were at the top of the main staircase, and turned towards the area where the military attaché had his office. Walking quickly across the floor, they gathered around the safe in the corner. The keys the embassy messenger held opened it easily. Inside were a variety of documents and items, one of them a black bound leather book. This was the American diplomatic codebook. Alongside it was another book, which contained its super-encipherment tables. The four men took the two books, did not touch anything else and left the way they had arrived. They took the books to the SIM headquarters, photographed each page of the contents and then replaced them in the embassy safe before dawn broke over central Rome.

The Italians later said that they gave only rough versions of decrypted messages, based on the codebooks, to the Germans. Another Italian version, from Cesare Ame himself, says that they simply handed the two collections of photographs to representatives of the SS, Gestapo and German foreign ministry at their Rome embassy two days later. OKW-Chi's second-biggest intercept station by that stage of the war was at Lauf, the medieval town north of Nuremberg, where 150 of Wilhelm Fenner's men were on duty at any one time. Listening in to signals picked up by six intercept towers from as far away as Egypt, Lauf targeted the American embassy in Cairo as a priority. Wilhelm Fenner said that they had no success with the American diplomatic or military codes before this incident. However, Walter Fricke, the head of the Lauf intercept station, stated that they had first broken into the US diplomatic system in July 1941, though initially they could read only parts of it.

America's New Military Attaché in Cairo

The American State Department assigned a new military attaché to their Cairo embassy in October 1940. His name was Colonel Bonner Francis Fellers, a graduate of the Class of 1918 at West Point, who had previously served in America's embassy in Madrid. His new job saw him tasked with the duty of monitoring and reporting on British military operations in the Mediterranean and Middle Eastern Theatre. What the British did was to give Fellers access to their operational briefings, their front-line movements, and

intelligence information gathered from the Germans, Italians and even the Americans. Fellers was taken on tours of front-line units, he spoke to British soldiers and British commanders, he knew about the latest tanks and aircraft and equipment arriving in North Africa, and he had a pass that allowed him to visit the naval bases at Alexandria and Port Said. And every day he dutifully reported everything he learned to his superiors in the United States. His reports were read by President Roosevelt, the head of American intelligence, and the Joint Chiefs of Staff. Of course, what he didn't know was that because of the nocturnal burglary of the Rome embassy, his signals from Cairo to Washington could be read by both the Germans and the Italians. The latter estimated, in their own words, that within eight hours the most secret data on British strengths, positions, losses, reinforcements, supply, situation, plans and morale was in the hands of German and Italian military. Fellers himself was a good soldier, a good patriot, and concerned about security. Twice he flagged up the security issue about the Cairo embassy codes with Washington, and twice was overridden.

Because Fellers' messages provided detailed information about troop movements and equipment to the Germans, they proved vital to the German war effort in the Mediterranean. That was the line that OKW-Chi gave when it justified to the Reich Security Main Office the huge expenditure of men and material over eight months following Fellers' information. Rommel's headquarters sent messages to Berlin insisting that the source of the information be protected from external interception. Wilhelm Tranow and his teams at the B-Dienst were very keen to access Fellers' messages, as they alerted the Kriegsmarine to British convoy operations in the Mediterranean, which centred on efforts to re-supply Great Britain's crucial island fortress between Italy and North Africa: Malta. So beginning in January 1942, information about the numbers and condition of British forces was provided to General Erwin Rommel, who, obviously, used it to plan his offensive and defensive operations. The Germans referred to Fellers as '*die gute Quelle*' or 'the good source', while Rommel referred to him as 'the little fellow'.[1] That both of these descriptions in English and German were rhyming puns on the name of the well-meaning American did not escape either Wilhelm Fenner or Wilhelm Tranow.

How the German Cryptanalysts Read Colonel Fellers' Messages

In late summer 1941, a messenger arrived at the German Wehrmacht signals intelligence headquarters at the Tirpitzufer in Berlin. The man who delivered the package of documents said simply 'we've had luck', Walter Fricke recalled later.[2] The Americans used substitution tables, and the practical work on them during the war showed that American cryptographic personnel were often so careless that they facilitated the work of the Germans. The pages of the codebook that arrived with the messenger had clearly been photographed – it was the pages of the book 'borrowed' from the American Embassy in Rome. The US military attaché's systems employed a five-letter code with only 8,000 groups, each of which represented a different word. There were two principal codes, the Intelligence Code and the Confidential Code; in the former, ten substitution tables were used in which vowel replaced vowel and consonant replaced consonant. The indicator denoting the recipient was placed behind the date group, and was sent in clear. When it came to making a break in the text, so that the recipient deciphering the message knew to switch substitution tables, another indicator would be placed in the text. Despite the use of ten tables, there were frequent cases of repeated words and different phrases, which Fricke and his team called 'crocodiles'. Another method that they used to spot frequently repeated words was in the case of proper names, such as Alexandria or Port Said or Suez. These could not be represented by cipher groups so had to be split up and spelt out individually. This also happened with the names of planes and ships and weapons: but foreseeing this, when these were used, a 'repeater' group appeared after the word in question. This meant that if and when the word was used again, it would be represented by one word group representing everything.

'Patience and watchfulness are the supreme rule in the interception and cryptanalysis service,' said Fricke. 'It is always a question of waiting for the mistake the enemy will make some day … and he will make it some day with absolute certainty.'[3]

By 1942, Fricke and his team were already reading much of the content of Fellers' messages, and by the spring of that year, all ten substitution tables could be read in their entirety.

'The most important was the Cairo-Washington link,' said Fricke.[4] 'To the great delight of the German cryptanalytical service he [Fellers] was extremely talkative … he did the Germans a two-fold favour … abundant material and excellent intelligence. … (the work to decipher the messages) was carried on

feverishly, like an exciting novel where you want to reach the end. The dead letters of a cipher group take on life and become people, tanks, infantry regiments or friends or foes.'

One factor that particularly helped the Germans was that at the end of each week, Colonel Fellers would dutifully include a shipping report of all the vessels transiting the Suez Canal. The ships' names were repeated, sometimes three times, and a ship that one week would be 'outgoing' – i.e. entering the Suez Canal at the north – could be 'incoming' the following week as it sailed in the opposite direction. The reports appeared bang on time at the end of the week, and the dedicated decryption teams who worked day and night at the monitoring stations at Lauf and Treunbritzen worked on each message until, they said, it came together like a mosaic.[5]

Fellers was the perfect source. He was hard-working, dedicated and ambitious. He was a natural narrator. He did not like the British very much – he was one of a coterie of senior American officers who despised the British Empire and its imperial military and naval advocates, whom they saw as lofty and conceited. And he was aware of just how much the British needed American assistance, so he knew they would give him, in turn, as much help as he asked for. When an investigation convened in 1944 to try to work out quite how much information Fellers had given the Germans, the colonel himself said that 'if I was going to be a good observer and write good reports I'd better report what I saw myself'. So in his peregrinations around the British operational sector, and their front lines, he talked to as many soldiers and civilians as he could. As he said about the battlefront, here 'it wasn't difficult to learn a great deal'.[6]

If a signals intercept and or intelligence officer could imagine their perfect source, it would be Colonel Bonner Fellers. Every day he wrote long and downbeat radio messages in which he described everything he could to Washington. Then he took out his copy of the American diplomatic code – his 'Black Book' – and dutifully enciphered them. How many new M3 tanks had arrived with the British 7th Armoured Division – the fabled 'Desert Rats'? Was their frontal armour going to be capable of withstanding direct hits from a Panzer III's 75mm gun at 900 metres, unlike that of the Valentine, Crusader or Lee? What was the cargo distributed among the different merchant ships en route to Malta in the next convoy, and, crucially, did they contain fuel oil or aircraft spares? How many cruisers or destroyers were to escort the convoy? How many twenty-five-pounder shells did each

unit of the British Royal Artillery have in reserve behind the front line? Was the morale of the Australian division really as low as reported? Were food supplies getting through from Syria, and what was the state of health of the South African Division? Fellers told the whole story. After he had encoded the signals, he filed them with the office of the Egyptian Telegraph Company in Cairo, and then they were transmitted across the Atlantic to Washington. And within an hour they would be in German hands, on their way to German cryptanalysts' desks. They would be picked up not just by 621 Company behind Rommel's front line, but also by Captain Feichtner's Luftwaffe signals intercept unit outside Athens. Anything that could not be broken straight away was sent to the OKW-Chi station at Lauf. So in another two hours, they would be cracked into readable English. They were then translated back into German. One copy went to Rommel's headquarters, another to the RSHA, another to Göring, one to Himmler and one to Field Marshal Keitel and Hitler himself. The fastest decryption of one of Colonel Fellers' telegrams was forty-one minutes. Within an hour or two at most, they would be broken into readable text, ready to be retransmitted in a German code. Thus, a few hours after Fellers' messages were sent, the data would be in Rommel's hands. Dr Herbert Schaedel at OKW-Chi was one of Wilhelm Fenner's archivists. He remembers that 'the whole … military infrastructure went crazy … to get all the telegrams from Cairo'.[7]

It was very easy, he said, to find Fellers' reports amidst the electronic traffic: he had obligingly coded them and marked them for MILID WASH (Military Intelligence Division, Washington) or AGWAR WASH (Adjutant General, War Department, Washington), and signed FELLERS. Schaedel later recollected that Rommel, each day at lunch, knew exactly where the Allied troops were standing the evening before.

•••

On 7 December 1941, the day of the attack on Pearl Harbor, Rommel's Africa Panzer Group started to retreat west and southwards from near Tobruk to Tripolitania, so he could regroup with Italian forces. Close to his headquarters were the trucks, half-tracks and motorcycle sidecars of Captain Alfred Seebohm's 621 Company. The British were, in the words of Rommel's chief of staff, going through one of their periods of displaying a total absence of radio discipline. They were not even changing their unit radio codes or

call-signs. Colonel, later Major General Siegfried Westphal said that the British were quite broad-minded in making speeches during combat, and the Germans had the possibility of taking important conclusions from these speeches. On 21 January 1942, helped by Colonel Fellers' latest report which told him that British armoured units had withdrawn from out of the line in front of him, Rommel attacked. He took the British off guard. He advanced 300 miles in seventeen days. And still neither the British nor the Americans suspected what Rommel knew, and whence it came. Colonel Fellers, *die gute Quelle*, was not slow in keeping Washington updated with Rommel's advance towards Cairo. On 29 January he broadcast a complete breakdown that listed the entire strength, and deficiencies, of the British armoured corps in the whole Middle East. Each Valentine and Crusader and Lee tank, the unit it belonged to, how much petrol and ammunition it had, the readiness of the units using it, were all in 'the little fellow's' telegram. Then he learned, from a disgruntled British cavalry officer who saw the British tanks in his unit being replaced with stronger American-made M3 medium tanks, that the US armour with its bigger guns, thicker armour and higher speeds would enter combat on the Allied side after the middle of February. So on 6 February he sent his daily telegram.

This time he described how the British and the French Foreign Legion had established a defensive front line, protected by minefields, that stretched all the way from the Mediterranean to the oasis at Bir Hakeim. From that line, the British intended to launch a decisive counter-offensive. Rommel had 560 tanks and 250 old Italian ones. The British had 700. Fellers' dispatches said that the Allies were about to attack. So the Desert Fox pre-empted them, and on 26 May he attacked south. He ran parallel to the British defensive line, drove south around Bir Hakeim, and then circled north behind the British line. And less than half a mile behind him came his precious signals company, Company 621. But then Rommel's logistics supply line over-stretched itself, his attack slowed down, and he stopped dead in the sand.

As everybody from Hitler, Rommel and Colonel Fellers to all of OKW-Chi and the B-Dienst knew, the focal point of British success in intercepting the German and Italians' Mediterranean supply convoys was the island of Malta, situated in between the far south-western 'toe' of Sicily and Tunisia. By mid-1942, it was under constant daily attack from the air and the sea. In May and June alone, the Germans and the Italians dropped 9,000 tons of bombs on it. Colonel Fellers' telegrams ricocheted daily over to Washington,

predicting that, if sufficient aircraft, food and supplies of fuel oil didn't reach Malta, the island would surrender by August. If it did, Rommel's army would have an uninterrupted chain of supplies, and aircraft to support him. He would be able to drive to Cairo, and the Suez Canal; if he took that, and the port of Alexandria, the German army could push south to the key Persian oil fields. The Kriegsmarine would control the Red Sea and access to the Indian Ocean, the Third Reich would have Britain's oil, and the war would be effectively won. Malta was vital.

And so in June 1942, the British decided to sail two important convoys simultaneously to Malta, one from Alexandria in the east and another from Gibraltar in the west; the operations were respectively codenamed *Vigorous* and *Harpoon*. It was vital for the operations' success that as many German and Italian ships, submarines and aircraft were either paralysed or put out of action before they could get near the convoy. The Royal Air Force would bomb airfields in North Africa and Sicily, and British special forces, including the Long Range Desert Group, or LRDG, and the emergent Special Air Service, or SAS, would stage long-range raids behind German lines on airfields in Cyrenaica and Libya. To the absolute astonishment of Rommel's headquarters, OKW-Chi and the B-Dienst, Fellers reported this in detail. Parts of the German intelligence establishment started suspecting that he had to be a double-agent, broadcasting fundamentally flawed information. But no. His cable, No. 11119, dated 11 June, was intercepted in both Rome and Lauf, and by 621 Signals Company:

> NIGHTS OF JUNE 12TH JUNE 13TH BRITISH SABOTAGE UNITS PLAN SIMULTANEOUS STICKER BOMB ATTACKS AGAINST AIRCRAFT ON 9 AXIS AIRDROMES. PLANS TO REACH OBJECTIVES BY PARACHUTES AND LONG RANGE DESERT PATROL.[8]

The LRDG, French commandos and the SAS, along with local resistance groups, duly attacked airfields on Crete and across Libya. One SAS mission arrived on the edges of a German airfield outside Bizerte in Tunisia, and as their Willis Jeeps drove onto the runways, floodlights snapped on from the aerodrome's buildings. Machine guns opened fire. The Germans were waiting for them. And Operation *Harpoon* and Operation *Vigorous*? Two ships from the former convoy arrived in Malta; the latter turned back after losing eleven

vessels from the convoy. But Rommel had suffered from over-confidence – when Fellers' broadcast in one of his telegrams that the 'British would crack under one last blow,' Rommel decided to drive all-out for Alexandria. So he did, trying to drive the British Eighth Army back into Egypt. At the end of June 1942, his army was ninety miles from Alexandria, one stop before Cairo and the Suez Canal.

Although it would seem tempting to blame Colonel Fellers for appalling lack of radio discretion and discipline, in his defence he did protest to the American State Department about the insecure codes he was made to use. In one of his own telegrams, on 2 February 1942, he stated that '[I] believe that code compromised', but Washington insisted the code was secure.[9] Bletchley Park saw intercepts both from the Luftwaffe and the Heer which claimed that the Africa Corps was receiving regular information from 'an Allied military source in Egypt'. The British were suspicious of Fellers. On 12 June they informed the Americans that their defence attaché was almost certainly the source of high-level leaks to the Germans, albeit unwittingly. It was a partial bluff. The Americans fell for it, Fellers changed his codes on 29 June, and Rommel's best source of information on his enemy's dispositions and intentions dried up. To many people's amazement – including the Germans' – Fellers was not disciplined for the fact that his reports were intercepted, instead he was transferred, decorated with the Distinguished Service Medal, and made a brigadier general. His successor simply used another code that the Germans could not read, a military cipher encrypted on a Hagelin M-209 machine.

The citation for Fellers' DSM was based upon his clear and accurate analysis from Cairo. Although, as one colleague in the Office of Strategic Services claimed, he was the 'most violent Anglophobe I have ever encountered', his reporting about the British Eighth Army found favour in Washington. One signal of his bears repeating in full:

> *The Eighth Army has failed to maintain the morale of its troops; its tactical conceptions were always wrong, it neglected completely cooperation between the various arms; its reactions to the lightning changes in the battlefield were always slow.*[10]

Despite this, Fellers and his reports had a marked and extensive effect in bringing much-needed American supplies and troops to help the British in

North Africa. Throughout the time of his posting in Cairo, Fellers' argument was simple: more American help for our allies, with more American weapons, more American troops, and now. In Washington, his stance on US support for the British flew in the face of what the US Joint Chiefs of Staff wanted to do. A North African landing – as Operation *Torch* would be – was then considered out of the question because the Americans, as early as 1942, were considering an operation called *Bolero*, which was a grandiose plan for an early invasion of Europe. President Roosevelt was a firm supporter of Fellers' reports, and was influenced by them, leading the Chief of the General Staff, General George Marshall, to write to Roosevelt to say, 'Fellers is a very valuable observer but his responsibilities are not those of a strategist and his views are in opposition to mine and those of the entire Operations Division.'[11]

Despite this institutional opposition to his former attaché, Roosevelt invited Fellers to the White House upon his return from Cairo. Again, Fellers argued for what he called 'robust and expeditious' reinforcement of British forces in the Middle East. The final irony was that, for a man who unwittingly so helped the enemy, Fellers' analysis of the Middle East situation was such that Roosevelt eventually decided to support the Eighth Army, and commit to Operation *Torch*, the American invasion of North Africa.

The End of 621 Company

In mid-summer 1942, in the month of July, out in the desert behind Rommel's front lines, Captain Alfred Seebohm was barely half a mile behind the forward troops. He was on a spur of high ground called Tel el Eisa, a station on the railway line near El Alamein. The site was an excellent position, on high ground, well placed for interception and for communication both with the liaison team operating with Rommel and with the central evaluation unit. But the British spotted the unit after flying over with a reconnaissance Spitfire; they also claimed to have intercepted the Enigma messages that the unit sent to its evaluation unit, normally stationed several miles behind its position. On the night of 10 July 1942, Australian troops led a raid on 621 Company. In the opening phases of the attack, two platoons of Italian troops, which were in the same position as the signals intercept unit, instantly fled: the Australians had Bren Gun carriers, mortars and anti-tank weapons, and at the moment they attacked, Captain Seebohm

was visiting his forward platoons; wounded, he died two days later in a hospital in Alexandria. Seventy-three men of the intercept platoons were captured, along with their equipment and a large quantity of documents that showed what the unit had done. While Rommel was furious that the unit had been wiped out, it was difficult to imagine them being stationed anywhere else except close to the front, or they would have been of no operational value. But the loss of seventy-four very experienced men, as well as the British capture of their documents, meant that the unit had to start back from the beginning. One of the officers on Rommel's intelligence staff was Colonel Hans-Otto Behrendt, and he described the capture of 621 Signals Company as a 'catastrophe (with) serious consequences for Panzerarmee Afrika'.

•••

By early summer 1942, the naval Enigma 'blackout' at Bletchley was just one factor that had helped create a tactical and strategic 'perfect storm' for the Germans. On almost every front cryptanalysis was proving to be of strategic assistance to the Third Reich. Helped by Colonel Fellers' signals, the Africa Corps had defeated the British at Mersa Matruh, bringing Rommel 150 miles from Alexandria. On the Eastern Front, five Russian armies were surrounded near Kharkov, as the Germans launched Case Blue, the operation to take Stalingrad as part of their sweep to the Caucasus.[*] In London, there was no denying the war was going the way of Germany; Churchill barely survived a vote of no-confidence in the House of Commons, and on 3 August, the British prime minister was forced to tell Stalin that there would be no 'Second Front' in 1942.

---

[*] German codebreaking and signals intelligence operations in Russia are presented in Chapter 15.

Chapter Fifteen

SIGNALS INTELLIGENCE AND CRYPTANALYSIS ON THE RUSSIAN FRONT

Long before their invasion of Russia, the Germans had been working hard to establish Russia's signals intelligence and cryptanalytical capability. The signals intelligence agency of the regular army, the Oberkommando des Heeres, was only formally created in 1939, and as noted previously, between 1940 and 1942 was called Inspectorate 7/ VI. Thereafter it was called Oberkommando des Heeres/General der Nachrichtenaufklärung (OKH/GdNA), or GdNA for short. It took over much of the coverage of purely military signals from OKW-Chi in 1939.

One man who worked for the GdNA was Lieutenant Alexis Dettmann. He had begun working as a young officer in signals intelligence in 1935, picking up Russian signals at fixed radio receiving stations at Treunbritzen and Juterbog, in north-eastern Germany.[1] In these early, pre-war days, the majority of the work that he handled was from the Soviet Union's Ministry of the Interior, known as the NKVD.

The letters stood for the People's Commissariat for Internal Affairs, or Narodnyi Komissariat Vnutrennikh Del. It was originally established in 1917 during the Russian Revolution and its mandate was to be the police force of the new Communist regime, guarding the borders of what would become the

new Soviet Union and running the country's vast prisons and labour camps. By 1934, its duties had been expanded to cover everything involved with state security. Such diverse matters as prisons, the security of railways, railway stations, government buildings, the road network, borders, river crossings and centres of economic production like mines and state farms, repression of the Communist Party's enemies and firefighting all came under the jurisdiction of its several directorates. It was in charge of political education and indoctrination of Communist Party ideology at every level of the army from general down to private, imposed via a network of political commissars. It also ran such arcane outposts as sniper courses, as well as the training of messenger dogs and carrier pigeons. The counter-espionage umbrella organization called SMERSH, from *Smert Spionam* – translatable as 'death to spies' – was formed out of the NKGB, a sub-division of the NKVD. Its soldiers helped carry out the Great Purge under Joseph Stalin from 1936 to 1938, in which an estimated 600,000 soldiers, army officers, Communist Party officials, peasants, teachers, doctors, farm managers and members of the intelligentsia were shot, gassed, starved or beaten to death, mainly by NKVD units led by Nikolai Yezhov. Ironically, he was also eventually killed in the purge. He was succeeded by Lavrenty Beria.

From 1935 to 1937, the German signals analysts discovered that 70 per cent of their intercepted radio communications and radiograms from Russia were of NKVD origin, and these were considered far more interesting than the very simple signals sent by the Russian army and air force. There were three main reasons for this. Firstly, the Ministry of the Interior was responsible for the physical security of Soviet territory, and its troops were stationed all along the borders of the Soviet Union, so they saw everything; secondly, the NKVD reported *everything* both upwards and downwards in a direct hierarchy of operational command; and thirdly, they reported on the three areas which were of most interest to any foreign armed force, such as Germany, which had plans to invade the country.

The first of these three areas was military security, as in the numbers, designations and mission of army and air force units stationed along and behind the country's borders; the next was infrastructural security, with constant reporting on railways, roads and air links; and the third was political and economic security: which army unit could be considered reliable, and what the country was or wasn't producing, where, and what it needed more of. By intercepting and trying to decrypt the signals of the NKVD, the

Germans could thus deduce the military, political and economic status quo inside the country in which they were planning to operate.

By 1937 the Germans were intercepting and reading NKVD radio messages from their fixed intercept stations at Königsberg, Breslau and Treunbritzen, and their primary targets were signals emanating from the Soviet interior ministry control stations. There were two at Leningrad and Murmansk in the far north, three in the crucial ports and cities of Odessa, Novorossijsk and Sukhum on the Black Sea, and others at Baku in the Caucasus and at Tashkent in the Central Asian region of Uzbekistan. In the centre and south of the Ukraine, the German targets were Minsk, Kharkov and Kiev. If their signals intelligence could monitor, intercept and decrypt radio traffic from NKVD units stationed along this vast line, approximately 1,600 miles long, which ran from the Arctic Sea in the north to the Black Sea in the south, they could make an assessment of the state of military readiness inside the Soviet Union.

The Germans got a good lead-in to Russian systems because they started early, and because before the war Russian signals were in their infancy, and the Germans had followed their development. The first radio signals coding system they used was called PT-35, or 'Talk Table 35' which was called this to reflect the year of its introduction. The basis of the code was keys made up of 'system squares' of numbers, ten vertically and ten horizontally; these often remained in service for up to two years. So each square consisted of 100 random numbers, and was issued to unit radio officers. Three or four squares would be used alternately at any one time in any military district, employed in tandem with a book of encipherment tables. An indicator was attached to the enciphered transmitted text, consisting of two figures. The first figure indicated which ten-figure line in the system square provided the page and line number in the encipherment table, while the second figure delineated the different system square to use to decipher that particular day's message.

Four years later, in 1939, the PT-39 was introduced, containing 'switch groups', which told the recipient whether they should read the letters or the words in a particular message. Early in 1942 the PT-41 came in, and this too was based upon system squares, with switch groups as well. Ninety-eight cells – or squares – out of the 100 on the table had two meanings, and there were two switch groups to tell the operator which number to take from the square in question and compare it with his encipherment tables. It went without saying that these system squares were laid out in Cyrillic script.

•••

From the outset, Dettmann was an example of how a capable army can put the right person into the right job: despite his junior rank as an officer, his abilities and responsibilities were greater than the number of stripes on his collar. He saw very quickly that by the simple expedient of listening to what an enemy was saying, as often as possible and in as many different locations as possible, an intelligence picture of an opponent could be painted. The people required to construct this picture, said Dettmann, needed certain skills:

> Cryptanalysis calls for good linguistic knowledge on the part of translators, and translator decrypters, and good mathematical knowledge on the part of analysts but also presupposes in both cases an adequate general background, quick comprehension, adaptability, persistence, mental altertness, a certain amount of imagination and an indefinable knack.[2]

He was also firmly convinced that cryptanalysts were best if they were not required to form part of a military hierarchy:

> Civilian employees [were even better and] had no need to do anything military, drill, roll call, guard duty, their entire time and energy could be devoted to one task, cryptanalysis. [Military] Administrative authorities thought that the number of personnel, not the quality of personnel, was the all important factor of cryptographic success. This layman's view regarding the 'Black Art', as cryptanalysis was called, resulted in very little attention being given to the actual difficulties while the supreme command not merely regarded disagreeable results of encipherment and evaluation with scepticism but rejected them as untrue and tendentious reports.[3]

Regiments of NKVD troops were stationed along the huge geographical chain stretching across the Soviet Union's western border, and they were a separate entity from the RKKA, the abbreviation used for the Red Worker and Peasant Army, most commonly shortened to 'Red Army'. Standards of education among the officers were higher, and some of the NKVD officers spoke foreign languages. The NKVD stationed regiments behind the front

lines as military defence, to prevent desertions from the army, and to stop the penetration of any foreign agents or troops; in real terms, before the outbreak of war in 1939, this meant anybody who was not from the Soviet Union and who did not have an authorized reason to be in a particular area. The NKVD were, simply, the paramilitary guardians of a brutal and repressive communist dictatorship. Their regiments safeguarded everything, the rear areas, railway stations, railway lines, roads, entrances to towns and villages, political headquarters, airfields and ports behind the initial front-line occupied zones.

The NKVD guaranteed the security of the army: when an army or army unit moved, the NKVD unit accompanying it moved too. So from intercepting the traffic of the NKVD units the Germans were able to ascertain which army units were moving and being stationed where. In addition, it guarded the country's railway system – German decipherments showed that before and during the war wholesale hijacking of trains, murder and robbery was commonplace on the Soviet railway system. The NKVD also controlled large sectors of the economic production by guarding state farms and factories, and they reported constantly on these economic and communications responsibilities.

Nor were the Germans impressed by Red Army signals preparations prior to 1939. For instance, the Russian armed forces would broadcast widescale radio transmissions in the days and weeks leading up to their annual 1 May military parades; the Germans intercepted these signals, which told them the number of troops, the names of visiting high-ranking officers and the types and numbers of aircraft involved.

Hans Eick and Luftwaffe Signals Intelligence before Operation *Barbarossa*

Colonel Hans Eick was no stranger to Russia. The fifty-one-year-old German officer had been there long before Operation *Barbarossa* began on 22 June 1941. His knowledge of the Russian language, its people and its political ideology was more advanced than most of the three million or more German servicemen who were involved in the immediate phases of the invasion, whether as front-line soldiers and airmen, those operating behind them, or those providing support from Poland or Romania or Germany. Eick was born in 1889 in Wesermünde, on Germany's North Sea coast. His father was a director of the North German Lloyd shipping line, and his job took him and

his family travelling across the world. Eick went to school in Bremen, and then studied electrical technology until 1911, when he turned twenty-two.

Eick visited Norway, England and France with his parents, as well as the United States, where he and his family travelled in 1909. Keen, curious and interested in other people and new things, he was astonished not just by the racial segregation in the country, but also by the spirit of the entrepreneur. He won a swimming championship at the YMCA, and visited Fort Myer in Virginia, where the Wright brothers practised flying. One day he was invited to visit the General Director of the Westinghouse Electrical Corporation, and in the anteroom of his office he saw a framed picture on the wall. It showed a cowboy pointing his revolver, with the caption 'Live always so, that you can look every man in the eye, and tell him to go to the devil'. It was an image that was to serve him, he later said, as a rod and staff for his whole life.[4]

Returning to Germany, he joined the infantry when war broke out in 1914, and was wounded in the Argonne; coming out of hospital, he joined the German flying corps, at a time when military aviation was in its infancy. Based in the south-east of Germany, he flew missions over Russia until he and his observer crashed in 1916. He was unconscious when he was taken prisoner. He then spent the next two years in Russia as a POW, much of the time in chains in a series of jails and detention centres from the Caucasus to Irkutsk in Siberia. He tried to escape three times, and in 1918 was moved to the Lubyanka prison in Moscow, where for a month he was witness to his fellow-prisoners being led to firing-squads. The German embassy arranged for his release at the end of August, but he was not allowed to leave Moscow. By this time he had learned to speak, write and read Russian, as it was one of the few things he could do to keep himself occupied in prison; so he decided to flee the Russian capital, which he did on a pair of crutches on a hospital train which took him to Berlin. On his return, he visited his parents, and as soon as he was fit again, he borrowed an aircraft and flew over London. It was a moment of heady freedom, and exuberant liberation.

Eick had seen quite enough of Bolshevism, and appreciated the increasing danger that lay in what he called the materialization and exploitation of the Communist idea into practical reality. However, on his return to Germany, he found disunity, fraud and lack of character rampant in the aftermath of the provisions of the Treaty of Versailles, which he regarded as a gigantic injustice done to the German people. From 1920 to 1934 he worked as the director of a series of electrical firms, and when the political spectre of

National Socialism emerged in the early 1930s, he embraced it eagerly. But he almost as quickly rejected it, as he saw that, although the idea of a form of political economic and social unity sounded like a good idea in principle, in practice it was not so attractive. He had seen Communism at large and in the wild in Russia, and he knew what it was and what it could do. Nazism, he thought, was the same.

Once again, the spirit of flying came to his rescue: he joined the German Sportsman Pilot Society, where he worked off his feelings in the air, the only element in those times, he said, that was still clean. At a reunion of wartime pilots in 1934, a colleague persuaded him that perhaps his future lay with Germany's new air force, the Luftwaffe. So from 1935 to 1937, he started learning Russian formally, and passed his interpreter's exam. Word of this veteran pilot who spoke Russian reached Major General Wolfgang Martini, the officer who was putting together the Luftwaffe's signals intelligence units. Would Eick come and join them? The answer was yes.

Operation *Barbarossa* Begins

Hans Eick's first posting with the Luftwaffe Signals Intelligence Service was as a major with an intercept unit in Saxony, where he monitored Russian, Czech and Polish signals. Next came Breslau, then Hungary, where he added Turkey and the Balkans to the list of countries and regions which his unit monitored. After this, he returned to Vienna in 1940, and was given his own signals battalion to command, and a promotion to lieutenant colonel.

Then came Operation *Barbarossa*: on 22 June 1941, 3,800,000 German, Hungarian, Romanian and Italian troops crossed into the Soviet Union on a 1,800-mile front, the largest land invasion in the history of warfare. Eick and his units moved across the border behind the front-line troops, welcomed by the Ukrainians as liberators from Stalin's menu of atrocity, oppression and the ideal of collective farming, which for them too often translated into poverty and bankruptcy. But as the Wehrmacht and the SS swept forward like a vast, steel shovel, leaving behind them prisoners, burning villages, and a devastated Ukrainian steppe, so the *Einsatzkommandos*, or 'action squads' followed. These were in essence mobile killing squads, normally made up of SS and Gestapo men, German police officials, and sometimes local recruits, whose job was to follow behind the advancing front line, and round up, detain and kill Jews, NKVD collaborators, communists and partisans.

Meanwhile, Hans Eick was by this time involved in interrogating captured Russian pilots, and watched the way that Russian POWs were treated by the Germans: they were handled as inferior people by supermen. They died, he said, like flies. Thousands of them, however, escaped German custody, pouring back through the vast front line to their own people and their own army, telling all too clearly and explicitly what was happening to them at the hands of the Einsatzkommandos and the Third Reich's 'administration', which followed its invading troops. They were, Eick knew, simply seen by the Russians as another Cheka, which was the populist collective acronym for the different agencies of Stalin's loathed and feared secret police, which had then taken on a popular meaning for all the Russian secret police organizations that followed.* So the war, for the Russians, became a nationalist cause of salvation, determination, liberation and survival. And by the time the German army arrived outside Moscow in the freezing winter of 1941, the Red Army was proving it.

Flying missions in support of the three German army groups in Russia – North, Centre and South – were three air fleets, or *Luftflotten.* Attached to these were three battalions from the 1st and 4th Luftnachrichten Regiments, the signals and air intelligence units. The Heer, or army, had a similar arrangement. Each army group had a Kommandeur der Nachrichtenaufklärung, a signals intelligence regiment known for short as KONA. They operated in exactly the same way as did the KONAs in North Africa – there were five KONAs on the Eastern Front, plus various subordinate companies. They listened to everything – coded, non-coded, clear, open voice messages – and discovered that in combat the Russians often transmitted their messages in clear. They included the name of the sender and the addressee at the beginning of some of their messages, for instance, and frequently, the German air force and army men discovered, the codename of their senior officer or unit was that of an animal.

The KONAs included 'tapping troops' of three men who went behind enemy lines, into No-Man's-Land to intercept telephone lines. They discovered that the Russian habit of reporting everything to their superiors, of whom they were just as scared as of the Germans, meant that partisan messages always reported that something had just *been* done; when a big operation was being planned there was always radio silence. The German army and air force cooperated closely. While cryptanalysis was done far behind the front lines back in Germany and Austria, signals monitoring and

intercepts both for the army and air force were done in the field, following the front line as closely as possible, in a similar way to the operations of 621 Company in North Africa.

The distances covered were huge, and in many ways the vast size of Russia made it a not-dissimilar operating terrain to the Western Desert. Clear air provided excellent signals transmission, the units were constantly on the move, fighting swayed backwards and forwards, and everybody and everything seemed at the mercy of massive skies that sparkled with sun and spring rain, or throttled the ill-equipped German troops with freezing snow. By mid-December 1941, for instance, some of the Luftwaffe men in the forward intercept units near Moscow had started wrapping frozen socks around their hands, to stop the skin on their fingers from sticking to the sub-zero cold of the metal knobs on their radio equipment.

•••

After the beginning of Operation *Barbarossa*, said Alexis Dettmann, 'no foe learned faster than the Russians'. Cryptographic reports after 1941 showed two things very clearly – the increasing development of the economic manufacturing base in and around the Urals, and the assembly of large Red Army units behind the front line. Both were repeatedly ignored by the German High Command. The Russians, said Dettmann, had 'Time, Winter and Space at their disposal', and signals intelligence constantly decrypted signals that showed how the Russians were using, and were to use, all three to their own victorious ends, meaning that the Wehrmacht and Heer's signals intelligence officers considered the German High Command guilty of conscious underestimation of the Soviet army and air force before and after 1941.

What did the German Wehrmacht and Luftwaffe Learn from Intercepted Signals?

One factor that made signals interception much easier for the Germans was that the NKVD and the RKKA reported everything upwards and downwards, so parallel texts were in abundance. Every kind of military, civil affairs, economic and political activity was transmitted down to the level of private soldier, and up to the commanders of regiments and divisions. These

messages below, intercepted by both Luftwaffe and German army units, give an idea of Russian signals reporting, and how the precision of the messages gave German signals analysts so much information:[5]

> *Army message:* To the Chief of Staff of the 267th Infantry Division: the Command Post of the 1032nd Infantry Regiment is located in the woods 2.5kms north-east of Ivanovo – signed Regimental Commander Petrov.
>
> *Air force message:* to the commander of the 127th Air Pursuit Regiment – send a liaison officer to the staff of the 4th Air Army at Poltava. Signed – Ssablin [actual spelling possibly Tsaplin or Shapalin]
>
> *NKVD message:* on 12.8.44 at 0750 o'clock Red Army man Kosolov, Petr Wassiljevic was arrested at the south exit of the village Dolgaya. He had deserted the evening before …
>
> *Army message:* To the chief of staff of the 149th Infantry Division, enemy in strength of one regiment of infantry and tanks has broken into our position …
>
> *Army message:* To the commanders and chiefs of staff of the 172nd, 178th and 192nd Infantry Divisions, and the 73rd and 112th tank brigades, 172nd Inf Div attacks on 14.6.43 at 0403 o'clock with the 460th Infantry Regiment in the direction of Gorovok …

In the early days of the war German signals intelligence units recognized a message that was sending Russian aircraft to counter-attack the Germans who were crossing the River Danube in the Ukraine, and this resulted in the interception of the bombers. German fighters shot down 100 of them – in the first week after Operation *Barbarossa*, German aircraft destroyed some 2,000 Russian fighters and bombers, most of them on the ground.[6] There was then an almost uninterrupted flow of information about the supply chain for Russian troops, and the numbers of wounded and dead, the health of the living, morale of troops and desertions, all of which were noted with daily precision.

> *Army message:* The condition of health in the division is catastrophic. Dysentery of epidemic proportions, 379 cases to date. Request medical assistance. CO 164th Infantry Division.
>
> *Red Army Air Force message:* Aircraft recognition signals – on the 23rd

May dip the right wing twice, and during the night of the 23rd–24th short flashes by plane lights for a period of three seconds. Passwords: Challenge: *Tashkent*, or *Honour*. Answer *Kazakhstan*, and *Fame.*

NKVD message: to outposts 4,6,7,8 and 9, during the night of 4th–5th October the enemy dropped agents in the area 6211, 6212, 6311. Take measures to find them. CO 68th Regiment.

NKVD message: On the 8th October the lieutenant in charge of the 8th Outpost of the 68th NKVD Regiment reported the arrest of civilian Ivanovic Jersov, without proper papers, 25 years old, blue eyes, dark blonde hair, medium height, stocky, no special marks of identification, dressed in a green jacket, old grey trousers, black army boots.

The Russian Signals Intelligence Structure

The Eighth Section of the General Staff in Moscow controlled all matters of cryptography in the RKKA, army and air force, and a cadre of strictly observed Communist Party members ran recruitment by the NKVD, and also oversaw the cipher schools for personnel in Moscow and Tambov. A captured Russian captain who had attended these schools said that they provided no teaching about foreign cryptograms or cryptanalytical systems, except for brief examples to show that they existed. Instead great emphasis was placed on teaching history such as that of the 1914–18 war, and the successes and failures of the Battle of Tannenberg in August 1914. After 1943 non-Communist Party members were allowed to be employed, with training reduced from six to three to one month. Before 1943 the Eighth Section had sixty-five officers and men; afterwards there were only forty-four, as every available man was being sent to the front line. Although backed up by mathematicians and linguists, the section put very little emphasis on cryptanalysis.

During their advance in 1941 the Germans captured a significant amount of cryptographic material from towns, villages, airfields and aircraft, from the bodies of dead and living Russian officers, and from tanks, lorries and jeeps. Everything the Germans found, from the military or air force, was sent back to the KONAs or the nearest Luftwaffe base. Since, for instance, only one basic five-figure coding system with additives was being used by the Russian divisional-level staff across an entire army front, 500 miles long, the capture and decryption of one code and codebook meant the signals of an entire army

group could be read. So by late 1941 the Soviets realized they had to change their coding system. This was done by the two Soviet Union agencies that were in charge of using military cryptographic systems in order to secure their communications: the NKVD's Fifth Department, and the Red Army's Eighth Section, mentioned above. The latter was part of the main army intelligence directorate, the Glavnoye Razvedyvatel'noye Upravleniye (GRU, or Main Intelligence Directorate).

The Soviet military used two-, three- and four-digit codes, while substitution methods and additive sequences were used to encipher the most important four- and five-figure codes. The NKVD relied on figure codes enciphered with both substitution and addition methods, while partisan groups also used figure codes enciphered with additive sequences or transposed based on a key word. The diplomatic service used four-digit codebooks enciphered with 'one-time pad' tables: these were simply message forms where an encryption code and deciphering table were issued to diplomats to be used only once: if it *was* only used once, it was unbreakable. But the Russians got careless, and frequently used them twice or more. The Soviet Union's two-digit codes were used, initially, by the Russian army, the air force and the NKVD units. In the army, they were mainly used by army groups, armies, corps, divisions, and regiments; and by small independent special units such as combat engineer brigades, motor regiments, and artillery. In the NKVD, they were used on regimental communication close to the front, and from divisional level downwards. On the German side, when it came to decryption, the cryptanalysis of two-digit systems was done mostly in FAK units at the company level, but was also handled at the headquarters level of the Inspectorate 7/VI, and then later by the GdNA itself.

Codebreaking by the Luftwaffe and Wehrmacht in Russia

The Germans originally broke into the Red Army's main five-figure code in 1939–40 during the Winter War between Finland and the Soviet Union, with much assistance from the Finns, who had been breaking Soviet codes since the 1930s. The Soviet–Finnish war served as the equivalent of a training exercise for the German signals intelligence organizations: it was a real war, and the German signals units took every opportunity to analyse material captured by the Finns. One of Germany's codebreakers who benefited from this was Wilhelm Tranow.

The Germans also captured a copy of the codebook in their initial advance after Operation *Barbarossa*: in 1942 the Russians were still using it. They were able to use the allocation of unit call-signs and indicator groups in the book to establish the entire Russian order of battle and the location of their strategic reserves, as well as additional information that they gained from reading air force codes.

Tranow had begun working on Russian ciphers in 1933, and had then learned Polish and Russian, aiming to break the codes of both those countries in 1934 and 1935. At that time the Russian navy were using a four- and five-figure system, and, to the delight of the Germans trying to crack these encipherments, generally announced the movements of ships and troops and aircraft the day before an operation. By the time Tranow was into his stride working on Russia, they were using a five-figure code which was deciphered using not subtractor tables, but addition tables. These worked in the same way as a subtractor table, but obviously in reverse. The operator enciphering the message in front of him looked up the five-figure code for, say, 'destroyer' in his codebook. To encipher it, he went to the addition tables, and found the daily five-figure key group, which he added to the code word, not carrying additional figures over ten:

Five-figure code for 'destroyer' is: **27082**

Daily key code from enciphering tables is: **94165**

Added together without carrying gives: **11147**

This is the five-figure enciphered code the operator sends to represent the word 'destroyer'.

The five-figure basic codebook the Russians were using had 50,000 groups, or 50,000 five-letter clusters, each of which represented a word. Tranow and his colleagues broke it in spring 1940, and managed to discover the groups that stood for the names of ships or letters and punctuation; to do this they needed between eighty and 100 messages per day. Once they had broken this, the Russians introduced a double reciphering system, also based on addition, but one where the encipherment was re-enciphered, or 'super-enciphered'.

So the five-figure word code for 'destroyer' as above became 11147, but when super-enciphered, this was added to yet another five-figure group from a second enciphering table. Imagine this group for one particular day is 28841. Added to the already-enciphered 11147, with non-carrying addition, it gives 39988 as the super-enciphered code group for 'destroyer'.

Faced with this level of encryption, in 1940 Tranow left the Russian five-

figure code for a time, and concentrated on the four-figure one. He was short of personnel, war had broken out, he had the British Royal Navy's codes to attend to as a matter of urgency, and by that stage war with Russia was still more than a year away. But when the war with Russia did begin, his previous cooperation with the Finns meant that he could read a high percentage of their naval codes, which were identical in format to the ones used by their military high command. The encipherment table that used addition was based on code words from a book; Finland's cryptanalysts had told the B-Dienst in 1939 that this was almost certainly a book that was most likely either obtainable commercially, or was so standard to the Russians – in the same way the Bible might be for westerners – that any line and page reference in any copy of it would lead the operator to the same place, regardless of the edition of the book. So if, for instance, the day's reference was Page 56, line 8, word 5, the letters in this word would be replaced by figures, and these would be added to the coded groups in the message as the additive. The indicators used either at the beginning or in the middle of the message told the recipient the requisite page and line and word of the book in question.

Thus if the indicator was 145176, this meant that on page 145, line 17, word 6 could be found the word 'river'. In the accompanying encipherment table this would be given the figures 58344, for instance, and this would be added to the enciphered code words as an additive. The recipient of the message would, of course, have a copy of the same book for reference. So in fact, what Tranow and the Finns were dealing with was four- and five-figure super-enciphered codes using both additives and non-carrying addition. But what on earth was the codebook, thought he and his German and Finnish colleagues? What was so standardized and generalized in the Soviet Union of the late 1930s that every radio operator in the army or navy or air force or NKVD could be expected to have access to a copy of it? Then the codebreakers had a stroke of luck.

A German employee of the B-Dienst was, by chance, at that time living in the same house as the Russian military attaché to Berlin; as 1940 edged towards 1941, this officer either decided that it was time to return to Moscow, or was recalled. Having too much luggage, he left some books behind in the house. Once he had left, the B-Dienst staffer decided to help himself to some of them, which were sitting in a drawer. One of them was *The History of the Communist Party*. His discovery of this book, which couldn't be bought commercially in Germany, coincided with the Finns

telling Tranow and his colleagues that they thought this was the basis of the additive code. As a result, Tranow and his men managed to read into the entire Russian naval code, which helped them identify Russian minefields and naval movements in the Baltic, until the beginning of the siege of Leningrad in November 1941, when the codes were finally changed.[7]

By the end of the second week in August 1941, *Barbarossa* had been underway for seven weeks. The three German army groups had scorched across the Ukraine: Smolensk had fallen, four Russian armies were nearly surrounded near Kiev, Army Group North was heading for Leningrad, and in the south, German forces were on the steps of the Crimea. Nearly two-thirds of the Red Army's strength at the outbreak of war, or 2,750,000 men, had, the Germans stated, been eliminated. At least two-thirds of these were prisoners who had starved to death.

At the same time, German signals intelligence had broken sixty-nine different cipher mechanisms, including one code used by the Red Army's General Staff. This was the Russian five-figure system called OK40, or Operational Code 40, which was read into during the summer of 1941. This was a codebook with 25,000 letter groups, which were enciphered with an additive table of 300 five-figure groups; although the Germans captured the book at the start of the invasion campaign, the Russians had no idea their primary code had been compromised. Every division in the Red Army had copies of the book, their military organization and communications system was collapsing under the weight of *Barbarossa*, and nobody knew if one codebook with one unit somewhere on a front more than 1,000 miles long had been lost. So the enciphering tables continued to be re-used by the Russians. One characteristic of the system was that the first three figures of the code groups were either all odd, or all even: this made it extremely simple to spot messages that the Russians were sending in this code.

On 1 April 1942, two years after Tranow's initial successes with Russian codes, the Russians introduced a new five-figure military code, but according to the Germans the 'migration from the old to the new cipher was so faulty that within the first week it was possible to establish two thousand groups of the new code'.[8] They were to change the code again in early 1943, and assign separate codebooks and enciphering tables to their individual army groups, instead of having one common codebook for the entire front line from the Arctic to the Black Sea. The five-digit codes were used not just by the army and the air force but just as importantly by the NKVD, and as the campaign

in the Soviet Union developed, the German army was divided about whether breaking them represented a success or not. Lieutenant Colonel Mettig, the second-in-command of OKW-Chi, said that breaking them was the most outstanding cryptanalytic achievement by the cryptanalysts and signals intelligence personnel from the OKH. Some of the OKW-Chi and GdNA mathematicians said that as many of their officers and senior NCOs concerned with administration and organization knew little of cryptography, their opinion was invalid, and that the Russian five-figure codes even when broken yielded little. Yet others differed, as with every facet of German codebreaking in World War II. One cryptanalyst's technical meat was another codebreaker's professional poison: the Third Reich could listen very well, but it argued with itself in a bickering, paranoid way. So who was right?

Breaking the Soviet Five-Figure Codes

The Soviet five-figure code was broken chiefly by Alexis Dettmann, and there were several reasons why he and his team succeeded in reading into it. One was that the Russians had a tendency to transmit the same message several times, a habit that derived from the constant checking by superior officers of their juniors, as displayed in the examples of messages shown previously. Were the prisoners properly handled in the rear areas, did the fuel arrive, has the attack proceeded as planned, has the enemy broken through again, and where? As the Russians often used the same additives, or additive codebook, like *The History of the Communist Party*, it made breaking the five-figure and other codes much easier.

The next factor that helped the Germans was that they had captured the five-digit Russian military codebook, and almost two years after its capture in summer 1941 its enciphering tables still had not been fully replaced.

> It is interesting to point out that during the course of the war all the newly appearing versions of each cipher were captured through fortunate circumstances and always so soon that the originals were almost always in the hands of the cryptanalysts at the instance of their being put into use by the Soviets.[9]

Any codes that could not be broken at the level of the regiments or battalions in the field were forwarded back to OKH or OKW-Chi cryptanalytical units

operating either far behind the lines, or in Berlin. As mentioned, the Soviets used one-time pads frequently, where a one-off code was used to send a message where the recipient was the only person who knew the requisite encipherment: as the name implies, when used only once they provided very high levels of security. Inspectorate 7/VI considered them unbreakable. One NCO from a Wehrmacht KONA said that of the five-letter and five-digit codes used for operational orders, 'These were so-called Bloknot codes, which were only used once and were therefore unbreakable.'[10]

Bloknoten or 'blocknotes' was the German written version of a Russian word they had translated, which essentially meant a pad of paper, like a school block of leaves of paper, attached at the top but which could be flipped over. They were random sequences of numbers contained in a book and organized by numbered rows and columns and were used as additives in reciphering.

Knowing that successful cryptanalysis starts from the mathematical rule that the difference between two code groups remains constant if both have the same additive row applied to them, Dettmann also applied this rule to the breaking of five-figure codes. An example of a calculation for a 'table of differences' looked like this:

Code Group	**Additive**	**Cipher Group**
39214	20186	59390
98315	20186	18491
Difference		
41909	41909	

One of his most important cryptanalytic aids was therefore keeping a catalogue of 'differences', a numerically arranged table of the numerical variation between the most frequently used code groups, which could help break into them.[11]

German Cryptanalysis and the Strategic and Tactical Situation in Russia

Once the war in Russia began the German army and air force codebreakers continued to meet with some suspicion and scorn from their senior German commanders. One report on which both codebreaking agencies had worked

together was to estimate the approximate number of aircraft available to the Russians. The army said 11,000, the air force 10,500, both of which were relatively accurate. 'Absolute rubbish,' said senior German commanders.[12] In the winter of 1941–42, Inspectorate 7/VI learned, from extensive analysis, the makeup of almost every unit of the RKKA that was forming up east of the Urals – where, when, how big it was, the divisional number, the name of the commander, its garrison point, where and when and to which front it was to be committed. This information was to be confirmed by later developments at Kursk and Stalingrad, but at that point, the reaction by certain senior generals, including those from the Luftwaffe, was that these reports were 'nonsensical'.[13] However, by spring 1942 on the ground on the vast eastern steppe, several senior German army commanders took them very seriously indeed. After one winter in Russia, they knew what they were up against. As the muddy season had arrived the previous autumn, an annual phenomenon in Russia known as *Rasputitsa*, vehicles, men and the thousands of horses used by the Wehrmacht sank up to their stomachs in the liquid earth. In battle, the horses died alongside the men, leading a German soldier to write, 'A curious odour will stick to this campaign, this mixture of fire, sweat and horse corpses.'[14]

The Luftwaffe field divisions, which included the signals intelligence units, were in theory based on trucks, jeeps and half-tracks, but in reality almost all of them used horses for at least half of their transport. And Hitler, meanwhile, was so confident of a quick victory that the Germans had not prepared properly for fighting in winter; on 27 November 1941, Eduard Wagner, the Quartermaster General of the German Army, reported that, 'We are at the end of our resources in both personnel and materiel. We are about to be confronted with the dangers of deep winter.'[15]

And when winter came even the horses died from cold and lack of food: over 160,000 of them perished in December 1941 and January 1942 alone, and although the German soldiers could eat their dead four-legged colleagues, sometimes it was simply too cold. One German soldier wrote that Russia was a country where the winters were so severe that the 'axe rebounds as a stone from a frozen horse corpse'.[16]

•••

German cryptanalysis in Russia saw a level of cooperation between signals intelligence units that was not the same as in Berlin and Paris. The fixed and mobile units of the army and air force fed information backwards both to their unit evaluation centre and also to their agency headquarters in Germany. Their priorities were obviously the coded messages of the Red Army and of the enormous Russian political security police infrastructure that accompanied it, the NKVD. OKW-Chi, working for Wehrmacht High Command, cooperated with Inspectorate 7/VI, working for the Heer, while the B-Dienst had intercept units both in the Black Sea and in the Baltic, and the small and focused Pers-Z concentrated on the codes of the Central Committee of the Communist Party – or Comintern – itself.

In the opening days of Operation *Barbarossa*, one German infantry officer had said that the signals intelligence capability and the radio discipline of the Red Army were just as bad as each other. Soviet units treated the radio as a glorified form of personal telephone, and their codebooks used the most primitive comparative terms – tank, for instance, was encrypted as cow. However, although the Russians changed their codes and realized the necessity of modernizing their encryption systems, by spring 1942 the vast majority of Soviet enciphered messages were still written out by hand before radio transmission.

Dr Adolf Paschke, one of the German Foreign Office's linguistic cryptanalysts, saw that in terms of the different books used by the Russians in order to create cipher sequences and encipher the underlying code, it was thanks to their human error that it was possible to solve these and identify the books used. One of several examples of human error he highlighted was that Russian signallers who were responsible for enciphering messages had the tendency to reuse specific passages from the enciphering books, thus compromising the whole system. 'A particular instance deserves mention,' he said:

> It concerns telegraphic material of a total length of about two million digits. In the course of the work of solution it was established that it had been enciphered by means of five books which gave an encipherment sequence of about 5 million digits. An apparently hopeless case. And yet solution was achieved.[17]

German Signals Intelligence in the Siege of Sevastopol

By December 1941 the German assault on Moscow had stalled eleven miles in front of the capital, with winter in full swing. The Soviets then counterattacked in January 1942, but by March their offensive had run out. In the north, Leningrad had sat through the winter under siege by Army Group North, while Army Group Centre had shivered through December and January in slit-trenches from which they could see lights from Moscow. Hitler was determined to break through not just to the Caucasus but to the Black Sea, and so on 8 May 1942 Army Group South went on the offensive. The German Eleventh Army launched its attack all along the Crimean Front, aiming at the Kerch peninsula. After four weeks, the Germans began their assault on the tactical centre of the Crimea – the port of Sevastopol. And to support them, the Luftwaffe launched up to 1,000 individual sorties per day, with both fighters and bombers. To help assure the operational efficacy and security of these missions they urgently needed to know what the Soviet air force would do to counter their numerical air superiority. They knew that if they controlled the air over Sevastopol the battle would be half-way won, as the defenders would be unable to re-supply themselves with food, ammunition, men or fuel by air or sea or land. They would be cut off. So the Luftwaffe sent for a unit that could help them work out the Russian air force's intentions precisely, accurately, urgently and under fast-moving combat conditions. And if possible, in advance.

The signals intelligence unit that arrived was commanded by an officer who, like Hans Eick, had known Russia well, in all of its glory and all its atrocity-prone shame, long before *Barbarossa* had begun. His name was Captain Wadim Herold.[18] He had been born in 1916 in Iran, where his father was a merchant. His mother was called Olga Saposchnikova; she was a Russian woman from Siberia who had met her future husband while visiting her brother, a Russian cavalry officer stationed in Masshad in the north-west of the country. A city of religious pilgrimage, it was the centre of the spiritual faith that was based on the teachings of the fifteenth-century Lebanese scholar, Sheikh Bahai. But when Wadim was eighteen, his father died, and he and his mother moved to Germany, where she remarried; this time her husband was German. Wadim by now spoke fluent Russian. School and university in Germany led him to a career in electronics, a dalliance with National Socialism, and a decision to join the Luftwaffe.

By early 1942 Herold had crossed south-eastern Russia with his signals intelligence detachment, and on the second day of May they arrived outside

Sevastopol. The sky was slashed with the white of vapour trails and the black plumes of smoke from fires in the city; the air was filled with vast, dull booming thumps, like the trumpet of an outraged, oversized elephant. The noise, Herold quickly discovered, came from the vast siege mortars the Germans were firing into Sevastopol. Based on railway flatbed cars, three of them had a calibre of 60cm, twice the size of the largest battleship gun the German navy possessed. Captain Herold started to install his aerials, got his men to dig in, deep, and then got to work trying to intercept Russian air force signals.

•••

The siege of Sevastopol was about oil, and access to it. The Crimean peninsula was a vital stepping-stone en route to the oil fields of the Caucasus, and if it were not occupied by the Germans the Russian air force could use it to launch air strikes against the precious oil-production infrastructure at Ploiesti in Romania. Sevastopol was the major city on the peninsula, and by May 1942 the only one still in Russian hands. The Soviet naval base there was built around one of the strongest natural fortifications on the Black Sea, sitting on a limestone promontory at the tip of the Crimea which made any approach by land forces almost impossible. The city was very easy to defend, as the port at Severnaya Bay was surrounded by high cliffs which made an approach from the sea highly risky. The Russians had also built three separate circular and semi-circular rings of fortifications, reinforced with 188mm and 305mm battleship guns which could fire either out into the Black Sea, or inland. Some of these sat in reinforced concrete fortifications, and the German failure to take them was a primary reason why General Erich von Manstein decided to besiege the city for five months from February 1942, before launching attacks from land, sea and air against the Russians at the beginning of June. This combined operation was codenamed *Störfang*, or *Sturgeon Catch*.

The Luftwaffe played a vital role in this attack, flying 24,000 sorties and dropping over 20,000 tons of bombs in June alone, enjoying complete air supremacy over the Russians. This in turn enabled them to bomb the defenders of Sevastopol continuously, twenty-four hours a day; a large city of 400,000 people before the war, when the Luftwaffe had completed their role in Operation *Störfang*, there were eleven buildings left standing in it. The

German bombing of Sevastopol was heavier than that of London, Rotterdam or Coventry. To make it work as a tactical weapon, the signals intelligence units commanded by Wadim Herold were vital. The German fighters and bombers operated against Sevastopol from five main airbases set up at Eupatoria, Simferopol, Kitay, Sarabus and Saki, and this ring of airstrips was so close to Sevastopol that German Heinkel and Dornier bombers could just reach operational altitude before beginning their bomb runs.

The Luftwaffe signals units were based on each of these airfields, and through a combination of good equipment, techniques perfected across Russia, a secure operating environment where they were safe from counter-attack and did not have to move, and tough leadership, they excelled. The radio messages of every Russian squadron that tried to launch fighters over Sevastopol were intercepted before the Soviets were airborne; often Herold's men knew what the Russian air force was planning, and where they were a week before they launched an operation. They were flying inbound from airstrips on the Krasnodar peninsula east of the Crimea, and, knowing their movements, the Me-109s that protected the Luftwaffe bomber formations would divert to attack them, while the bombers dropped their explosive payloads on Sevastopol with complete impunity.

The Luftwaffe also made up for the limited amount of artillery available to the Germans: the Luftwaffe deployed six different bomber wings, and despite flying more than 3,000 sorties in one week, they lost only one Ju-87 Stuka to anti-aircraft fire. There was no Soviet air presence over Sevastopol, and Wadim Herold's men built up a comprehensive picture of any Russian attempts to interdict the airspace controlled by the Germans.

A Soviet officer called Colonel Ivan Laskin, commanding the 172nd Rifle Division in the northern sector, recalled:

> Bombers in groups of twenty to thirty attacked us without caring for their targets. They came in, wave after wave, and literally ploughed up the earth throughout our defence area. German aircraft were in the air above our positions all day long. The sky was clouded by smoke from explosions of thousands of bombs and shells. An enormous dark grey cloud of smoke and dust rose higher and higher and finally eclipsed the sun.[19]

The Germans killed, wounded or captured 118,000 Russians; Axis losses

among German, Romanian and Italian forces was 36,000 men, 28,000 of them German. The port fell on 4 July 1942. Captain Wadim Herold and his men stayed at their ring of airbases for two more months, then packed their aerials and their antennas, and advanced towards the Caucasus. They left behind them a completely destroyed city. Lieutenant Colonel Werner Baumbach, a Luftwaffe bomber commander, said just before the end of the fighting that in Sevastopol 'earth, water, rock fragments, steel and cement were intermingled with bleeding corpses. And yet the Russians continued to cling to their ground, their native soil, with unparalleled tenacity.'[20]

The German Sixth Army's Appreciation of Signals Intelligence at Stalingrad

Following on from the fall of Sevastopol, the German army began Case Blue, its operations around Stalingrad that began in autumn 1942. By this point, a clearly identifiable operational trend was beginning to manifest itself on the Russian Front in terms of cryptanalysis and signals intelligence. On the front line, in the mud and snow and dust of the trenches, German commanders up to the level of divisions and armies realized that they could trust the technical accomplishments realized by both the Luftwaffe and the Wehrmacht when it came to signals intelligence and cryptanalysis. This, however, was not reflected by a similar and commensurate trust back in Berlin or in the Führer's command post at the Wolf's Lair at Rastenburg in East Prussia. What this meant in strategic terms was that however accomplished were the cryptanalytical achievements on the ground, and however capable were regional German commanders, with their tanks and planes and infantrymen, of transforming this electronic intelligence into tactical reality, it mattered not at all if both efforts were being short-circuited from above.

•••

But by the end of November 1942, the German Sixth Army was cut off inside Stalingrad; by February 1943, they had been forced to surrender. Major General Wilhelm Arnold was a senior Wehrmacht officer who wrote a report about signals intelligence at Stalingrad on the basis of information given to him by General Paulus, commander of the Sixth Army, and some of his staff officers:[21]

> The intercept companies, consisting of an evaluation section and three platoons, were at the disposal of Sixth Army in the pocket of Stalingrad. In addition to these we had two intercept platoons of Fourth Panzer Army, thus a total of five intercept platoons. During the entire period of the encirclement the work of this reinforced intercept company was of the utmost importance to Sixth Army.

The surrounded army, said General Arnold, had no other means of collecting information about the enemy; for instance, a desperate attempt to send three fighters into the pocket on a reconnaissance mission had failed. As a result, Army G-2 (the intelligence component of the army) moved their entire section into the bunker of the intercept company's evaluation detachment. Fortunately, a large group of Russian interpreters had been assigned to the intercept company for some time:

> After the intercept stations had been installed, and the company had acquainted itself with the new assignment, we were able to determine the organization and approximate strength of the opposing Russian forces within a relatively short time. At first, Russian radio discipline was poor which enabled us to intercept and evaluate a series of clear radio messages. In the north-east sector, at least, this condition changed only when a new, apparently strict Russian signal officer was assigned there. He repeatedly prohibited all transmission of uncoded messages under threat of immediate execution of violators. However, even most of the coded Russian radio messages were deciphered by the intercept company quickly enough to be fully exploited.

During the preceding year Arnold's divisions had sent many specialists of the intercept company to their Army Group Centre for thorough training in deciphering the Russian three-, four-, and five-figure codes. That measure now yielded good results, as the well-coordinated employment of the five intercept platoons enabled them to present General Friedrich Paulus, almost nightly, with a complete picture of the changes that had occurred in the Russian lines during the day. This was a superlative achievement of signals intelligence and cryptanalysis in the face of intense and demanding combat conditions. In most instances the Germans were able to determine the Russians' intentions for the following day as well, and so push forward the

few tanks they had to the points where the Russians were going to attack. In the south and west of the Stalingrad pocket it was even possible regularly to intercept the exact Russian tank status reports.

On 12 December 1942, German General Siegfried Raus began his desperate relief thrust from the south through the Kirgize steppe towards Stalingrad, taking the heavily reinforced 6th Panzer Division, with its 200 tanks and assault guns, and the comparatively weaker 17th and 23rd Panzer Divisions, with many fewer tanks. Inside Stalingrad, according to General Arnold, several radio sets of the signal company, and a few sets of the intercept company were tuned in on the frequency channels of this relief force. General Raus' command channel, the channels of the forward divisions and the regiment in the main effort were monitored, and as the relief force continued its advance the voice communications of the armoured spearheads also became audible. Simultaneously, the intercept companies monitored the command channels of the Russian forces stationed opposite the forces of General Raus. This method of intercepting messages from both friendly and hostile forces provided the Germans continuously with a fairly clear picture of the situation. Intercepted reports of particular importance were passed on to General Raus by radio. Thus, the German signal units performed their duty at Stalingrad even under the most trying conditions, says the report. Paulus told General Arnold several times that 'their achievements helped the Germans materially to endure in the long and bitter struggle'.

As the German forces in Stalingrad struggled to hold the besieged pocket, in the winter of 1942 Inspectorate 7/VI was able to confirm with absolute precision the formation of new Russian armies to the east of Stalingrad, which were numbered sequentially from 62 to 69 and upwards. Given that each of these armies contained at least 40,000 fresh troops, these reports were operationally vital to the Germans. These signals analytics were constantly supplemented and confirmed but the German High Command could not make up their minds whether to believe them or not. As Alexis Dettmann wrote:

> Only when the 64th Army appeared, was Foreign Armies East of OKH allowed to enter the names of the other armies with question marks on the chart of the Red Army, and present this at the discussion at the Führer's headquarters without expecting to be exposed to wild insults.[22]

The Russians gradually improved their code security, however, and in the spring of 1943, they altered the indicator group system and split up their five-figure code into various front sectors. The Germans still focused on breaking them. By spring 1943, when Stalingrad had fallen, and with 208,000 German prisoners taken, Army Group South's push towards the Caucasus had failed. For the Germans in southern Russia, the war now became a series of constant retreats, encirclements, counter-attacks with too few men, too few tanks, too few supplies and nothing but tactical brilliance, determination and the raw urgency of self-preservation to keep them alive. They were prisoners of climate, too: in autumn there was liquid mud up to the axles of their vehicles, in winter rifle bolts that froze solid, and wind chill factors that took the temperature to thirty degrees below. Conversely, in summer there was choking dust and sand that clogged radio parts and machine-gun feed trays, while the men were always moving, fighting, moving, defending, mainly retreating, one eye on both horizons.

For the signals intelligence teams and the cryptanalysts it was hard to keep focused on the complicated maths and the requisite concentration needed for effective cryptanalysis. Even though the army's KONAs and the Luftwaffe signals intelligence units were not dug in on a desperate, snowy front line, firing shuddering bursts from an MG-42 machine gun at advancing lines of white-clad Red Army troops, they were not far away, and the tactical temperature of the front line dictated their moves, their retreats and their advances. There were hurried, sleepless days of frozen snow and boiling sun as they raced to set up intercept aerials, find radio frequencies, configure radio and Enigma sets to the correct setting, with their headquarters in Germany, Austria and Poland on the line demanding more, clearer, faster information. While not far away in front of them the vast Red Army, with time, winter and space at its disposal, hurled itself at the German behemoth that had dared set foot in Mother Russia. Yet the Germans did it. They kept reading signals, breaking them, evaluating new codes, focusing, and even when arguing amongst themselves – a perpetual failing – tried to keep looking clearly at the tactical and strategic context, sometimes hoping against hope for that decisive counter-attack, that last push, the new weapons that would help them push past Moscow and to a line near the Urals.

---

* It stood for the Extraordinary All-Russian Commission for Combating Counter-Revolution, Speculation and Sabotage, or *Wserossijskaja tschreswytschainaja*

komissija po borbe s kontrrewoljuziej, spekuljaziej I sabotaschem.

Chapter Sixteen

THE ENIGMATIC SWISS

Aided by a signals intelligence operation running at full steam, by early summer 1942 Germany's operational star was still in the ascendant. Their spring offensive around Kharkov had encircled two Russian armies; they were then still pushing towards Stalingrad, and meanwhile Burma was about to fall to the Japanese. Air Marshal 'Bomber' Harris launched Operation *Millennium*, the 1,000 Bomber Raid on Cologne – not only did it divert vitally needed aircraft away from the Battle of the Atlantic and aerial attacks on German submarine pens, it stiffened German civilian resolve to resist the Allies. The huge numbers of aircraft used enabled Luftwaffe signals intelligence on the French coast to track many Allied bomber and fighter operations over Europe. Rommel counter-attacked successfully in the desert, and by this point the Germans were also trying to read the codes of neutral countries. Their cryptanalysts realized that key neutral states such as Switzerland and Turkey could be playing all sides against the other, and horse-trading secret information with both the Allies and the Axis in order to protect and preserve their neutrality, and their security. The Abwehr were running a ring of agents in Switzerland, one of their priority targets being a group of Russian spies called 'The Lucy Ring'.* Meanwhile the signals traffic of the Turkish government and embassies in Ankara, London, Paris, Budapest, Moscow, Washington and Madrid provided cryptanalysts from Germany's Foreign Office, army headquarters and regular army agencies with

key information. In Hungary, a senior SS officer in Budapest was cooperating with a unit of Hungarian military codebreakers, and he repeatedly stressed that the best information the Third Reich gained from cracking the codes of neutral countries came from Turkey.[1] In truth, SS Sturmbannführer Urban from the RSHA, the Reich Security Main Office, was either buying information from the Hungarians that he cooperated with, or letting them do the work, and then simply forwarding the results of their endeavours on to Berlin.[†]

Yet if there was a close-run second place, it was taken by Switzerland. It was a neutral country with its status established at the Treaty of Paris in 1815, but during World War II it had cemented close economic relations with the Third Reich. The Swiss had done this to protect themselves from possible invasion, to continue to play their role as a neutral intermediary between various countries then at war, and because a keen sense of political-economic self-preservation in the national character drove them to forge alliances with the Germans, the Allies and other neutral countries simultaneously. Two of the biggest international organizations in the world were based in Switzerland – the International Committee of the Red Cross, or ICRC, in Geneva and the Bank of International Settlements, or BIS, in Basel. The former were the world's upholders of the Geneva Conventions, and the latter was an international financial clearing house. For instance, in early 1941, when the Yugoslav government realized that Yugoslavia was about to be invaded by the Germans, it decided to liquidate some of its national gold bullion reserves. It transferred these to Switzerland; the BIS paid it in United States dollars, and then transferred the assets for it to a series of banks in New York, Brazil and Argentina. It thus followed that both the Allies and the Germans were interested in the communications of the Swiss government.

The Red Cross was not just a vital source of information about what was happening to civilians and POWs across the Third Reich; its mandate of neutrality allowed it to visit and provide support to POWs on both sides of every front line. The effective price that it found it had to pay for this was minimizing the information it gave out about the ongoing killings of European Jews in Nazi concentration camps. It couldn't argue that it didn't know what was happening to Europe's Jews: the headlines of European and American newspapers could have told it. '25,000 Jews Seized in Southern France' said the *New York Times*, on 28 August 1942; '50,000 Jews put in

Nazi Prison Die Like Flies' was a headline in the *Washington Times Herald*, on 3 September 1943. '35,000 Jews Executed in Five Polish Towns' added the *New York Herald Tribune*, on 21 March 1943. 'Poles Report Nazis Slay 10,000 Daily' was another story, in the *Washington Post* on 22 March 1944.[2]

The organization's stance was clear:

> On 29 April 1942, the German Red Cross informed the ICRC that it would not communicate any information on 'non-Aryan' detainees, and asked it to refrain from asking questions about them. Information about the persecution inflicted on Jews did, however, filter out of Germany and the German-occupied countries, to reach the Allied governments, and some of this information also became known to the ICRC. In the summer of 1942, the International Committee of the Red Cross debated whether to launch a general appeal on violations of international humanitarian law. It prepared a draft, but decided in the end not to issue the appeal, believing that it would not achieve the desired results. The ICRC therefore continued with its bilateral approaches.[3]

That the ICRC might change its policy was a concern of the RSHA, and this was one reason why Göring's Research Agency took such a keen interest in overseeing the breaking of Swiss Enigma, at a time when three other agencies – Pers-Z, GdNA and OKW-Chi – were also expending valuable personnel time on it. For some of the signals about a variety of the activities and policies of the International Committee of the Red Cross were transmitted from the foreign ministry in Bern, to the Swiss embassy in Washington, using Enigma.

Making and Breaking Swiss Codes

The Swiss foreign ministry and defence ministry used different codebooks to encipher their radio messages, and although the Germans thought the level of complexity of these was low, what made them more straightforward to break into was the fact that many of the messages were sometimes transmitted in three of the four officially recognized languages of Switzerland, namely French, German and Italian, and so the foreign and defence ministries' codebooks appeared in all three. (The fourth official language was Romansh.) The Swiss military and diplomatic service also used commercial Enigma machines, considerably less complex than any of the models the German

navy, army or air force was using. The Swiss used a model called the Enigma K which had one disc, three rotors and a reflector, and no plugboard. Between 1938 and 1940 they purchased 265 of these machines and distributed them to their army, air force and diplomatic corps. The main difference between their machines and the German's was that when letter keys were depressed, the middle rotor moved forward one twenty-sixth of a rotation, and not the one on the right.[4]

The German army's cryptanalysts who worked on codes from France, Switzerland, Spain and Portugal were joined by both Pers-Z and by OKW-Chi in working on the Swiss Enigma system. GdNA intercepted Swiss traffic from an intercept station in Strasbourg, concentrating on the radio links between the Swiss foreign ministry in Bern and the Swiss embassies in Washington, London, Berlin and Rome. There was a very clear reason why the agency went to these lengths: 'The traffic of the Swiss Government provided cryptanalytic problems of moderate difficulty and owing to the fact that the Swiss served as representatives of belligerents in many countries, Swiss traffic was an important source of information.'[5]

The messages were either in French, German or Italian and numbers were sandwiched between X and Y with the figures 1, 2, 3, 4, 5, 6, 7, 8, 9 and 0 substituted respectively by the letters QWERTYUIOP, from the classical typewriter keyboard. Because the Enigma machine had no numbers on its keyboard, this meant that a thirty-six-letter alphabet now existed in which various letters – Q, W, E and so on – occurred twice. Up until late 1942 the internal settings were valid for a week and the same key was used for the links from Bern to Washington to London. The messages were sent in five-letter groups with the first four letters being the indicator, and some messages had the following coded designations: Saturn, Wega, Merkur, Helos, Nira, Urania. These were indicators of content, with Wega referring to shipping and transport matters, Saturn dealing with trade and Merkur with finance. The cribs used to break into some of the trilingual messages were straightforward, and on the link between Bern and Washington the following were used. For German codebreakers, a group of cryptanalysts used to breaking into the Royal Navy's codes and Russian NKVD cipherbooks, the Swiss messages were very far from challenging or complex.

'*Von Wanger für transport.*' (German)
'*Von Wanger pour transport.*' (French)

Erich Hüttenhain claimed that the Swiss Enigma machine was solved by his unit, and that as the wirings of the wheels only changed every three months they were not changed on all the machines on all the links at the same time. A message sent from the Swiss foreign ministry to their embassy in Washington DC at 11.59pm Bern time would arrive in Washington six hours earlier, at 5.59pm. If the Enigma settings were changed on a daily basis, the Bern operator would alter his rotor position at midnight, so any follow-up messages would be sent in the subsequent day's settings, but also, to account for the six hours time difference during which the Washington receiving operator would not have changed his rotor settings, the message was duplicated in the previous day's codes, giving the Germans a parallel text compromise. Not to mention the fact that it was in three languages.

There were three main methods of reading into the Swiss Enigma. The first was by using depths, which with the commercial Enigma meant messages enciphered on the same wheel settings:

> If 20 to 25 messages of the same setting are available, then the solution of these messages can be done in an elementary manner, through the columns of the encoded texts written under one another in depth. In this the reciprocity of the substitutions is made use of to a great extent. In the solution procedure no other characteristic of the machine is used. This is also valid for the elementary solution of the Enigma [with a plugboard]. After this elementary solution of the encoded texts the determination of the machine setting presents no difficulties.[6]

The second was by using a crib, and the third was by using the *E-Leiste* or E-List method. This was based on comparisons of the frequency of the letter E in clear text and in the cipher text the Germans were looking at:

> With the K-machine six different wheel orders are possible. The adjustable 'Umkehr' wheel can be set in twenty-six different positions. The periods of the three moveable wheels is about 17,000 steps, so there are therefore 6 x 26 = 156 different periods of 17,000 long respectively possible. If in each of the 156 different periods the clear letter **e** is encoded 17,000 times, then 156 rows of encoded elements results, each 17,000 long. All these rows of encoded elements are designated e-Leiste.

The explanation continued:

> The clear letter E appears in German with a frequency of 18%. If a German clear text encoded with the K-machine is moved through the e-Leiste and if in each position the corresponding encoded elements are counted, then the correct phase position will have the maximum cases of correspondence. In this the Ringstellungen [rotors] need not be considered. The E-Leiste need only be prepared once. The comparison of the encoded text with the E-Leiste would have to be carried out on a machine. In order to come to a positive conclusion in a reasonable time, then several machines would have to be used at the same time, even if one machine was capable of making 10,000 comparisons per second.[7]

It went without saying that even by the standards of deciphering Enigma machines, this was a complex way of doing it. It also remained largely theoretical, as unlike the British, the Germans had not introduced a bombe-style mechanical analysis for breaking other nations' Enigma systems. The German cryptanalyst later admitted: 'In Germany a practical solution with the aid of the E-Leist was not carried out, as in practice the method of solution from a part compromise was always possible.'

A far more straightforward method was that discovered by Pers-Z, Germany's Foreign Office codebreakers. They discovered that the Swiss used to include in their messages the machine settings for the next message, and so they could read Swiss diplomatic Enigma completely, for a considerable time.[8]

Yet according to an OKW-Chi report for 1941 the Swiss Enigma was partly solved thanks to a partial solution provided by Göring's Research Agency, the Forschungsamt. In order to do this, two Enigma machines were purchased and rewired according to the Swiss specifications and the results passed on to the Research Agency. It took between thirty and forty personnel to do this, and in the words of the deputy director of the Research Agency decipherment department, 'their main machine success was with the Swiss Enigma as long as the same machine setting was used over a longish period'.[9]

The expert at the Forschungsamt who really knew the Swiss Enigma was called Doctor Bruno Kröger, and during the war he solved several foreign cipher machines. The Swiss Enigma was first solved by processing several messages sent on the same key. The solution of these depths led to the

recovery of the wheel wirings and the further exploitation of the traffic, and when the wheels were rewired it was possible to recover the new settings by using assumed plain text-cipher text cryptanalytic attacks. It took, Kröger said, five to six workers roughly between one and six weeks to recover the wiring of the first rotor and then they could quickly recover the wiring of the remaining two. Eventually the use of enciphered indicators and individual internal keys for each message made it too costly to work on this traffic, so the Forschungsamt had to give up on it. According to Kröger this decision was made in early 1944. [10]

Apart from the activities of the Red Cross and organizations like the Bank of International Settlements, a third reason that the Germans were so interested in breaking into Swiss Enigma was that Himmler, Heydrich, Göring and the RSHA suspected that a network of senior Wehrmacht signals and intelligence officers and Abwehr officials were cooperating with the 'Lucy Ring' of pro-Russian agents in Switzerland, and that communication with them was even facilitated by the use of an Enigma machine, programmed to Swiss commercial settings. The Reich Security Main Office's fears went further: they suspected not just that two of the senior generals involved were implicated in pro-Russian espionage, but that these generals were in fact the department heads of two parts of OKW-Chi – and moreover that they were also involved in a plot to assassinate Adolf Hitler. The Reich Security Main Office were correct on all three counts, as later events would prove. The fates of the Führer and some of Germany's senior signals intelligence officers and cryptanalysts were now becoming dangerously intertwined at a moment when the Third Reich was fighting a war on two land fronts, as well as in the Atlantic.

---

* See Chapter 22.

† See Chapter 23 and the mention of the Yalta Conference here, which was an instance of the use of the SS and Hungarian signals intelligence cooperation.

Chapter Seventeen

RHUBARB AND RODEO

The objectives of Operation *Jubilee* were multiple. To be launched in mid-August 1942, the amphibious landing on the coast of occupied France would, said Allied planners, provide a practice run for the invasion of Europe. The RAF were desperate to engage the Luftwaffe in a large pitched battle in the skies over France or the Channel: they knew that any invasion of Europe would have to be preceded by Allied dominance of the air, and the destruction of the Luftwaffe. But in the first half of 1942, they had not achieved this, and so following their success in the Battle of Britain, the RAF was reduced to staging 'Rhubarb and Rodeo' raids over occupied France, small missions of two to six aircraft each that were designed to draw the Luftwaffe into aerial battle. The first was designated a fighter mission under cloud cover, the second a pure fighter 'sweep'. The tactic failed, as the Germans had deployed the new Focke-Wulf Fw 190 to the Western Front, and it was superior to the Hurricane and Spitfire. In the first half of 1942 over France and the Channel, the Allies lost 260 aircraft, the Germans sixty. Operation *Jubilee* aimed to create the conditions for the RAF's aerial showdown, and draw the German air force into the air to defend a major port on the French coast that the Allies intended to capture and hold. They chose Dieppe.

Secondly, the proposed landing would allow Churchill to show Stalin that the Allies were prepared, at least, to *attempt* a landing in France. The Russian

leader was demanding repeatedly that the Allies create operational conditions in the west that would see at least forty German divisions withdrawn from the offensives in the southern Ukraine. Thirdly, the Canadian leadership wanted to see their troops tested in combat. Fourthly, the British wanted to try to steal a German naval Enigma machine from the Kriegsmarine headquarters in Dieppe, and fifthly, the British were desperately keen to prove they could actually *win* something: late 1941 and 1942 had been a catalogue of tri-service defeats for them, from some of the Mediterranean convoys to Malta, North Africa, the Battle of the Atlantic, and Burma. These had then been topped off by Operation *Cerberus*, the successful Channel dash of the German capital ships *Scharnhorst*, *Gneisenau* and *Prinz Eugen* from the French Atlantic coast back to Germany. Dieppe was designed to redress this.

Deauville is a resort town on the coast of Normandy, in peacetime famous for its casino and its beach, a weekend destination from Paris. Lieutenant Martin Ludwig arrived in Asnières outside Paris in April 1942, while a team of his Luftwaffe signals intercept specialists were posted to Deauville, just one of several such units strung along the French coast. They were there to evaluate the traffic of the RAF and the US air forces based across the Channel, and provide as much early warning as possible of Allied fighter and bomber raids over occupied Europe, and any possible cross-Channel amphibious landings. Like the other Luftwaffe signals intelligence units, they specialized both in interception and decryption of signals. In spring 1942, the Americans, British and Canadians in England staged large numbers of exercises involving ground troops and air support units, and sent a lot of radio signals during and after them, many in clear, unenciphered speech and text. The Germans intercepted many of these, concentrating on establishing Allied radio frequencies, unit call-signs and messages sent from army units to the fighters supporting them in the air. Ludwig noticed that at the end of each exercise there was an 'umpire's meeting', normally held on a Tuesday, where the lessons from the exercise were discussed and messages duly dispatched about them. The British often sent these in clear text. A German company monitored these meetings, and given that there were up to 100 exercises taking place every month, there was a lot of radio signals material to work on. They established that a British army infantry battalion requesting air-to-ground support from the RAF or US Army Air Force (USAAF) would send this in a formulaic manner:

1. *Why is air support needed and what is the target and the threat?* (e.g. German armour in the village across the river at Grid Location xxx)
2. *How much support is needed?* (e.g. one squadron)
3. *When?*
4. *Special instructions* (such as to avoid dropping bombs on the village at location yyy as this was the headquarters of Allied troops)
5. *Is there any anti-aircraft threat in the target area?*

The Luftwaffe on the Atlantic coast and across France were also working on tracking Allied bomber units flying on day and night-time raids on Germany. Ludwig realized that a radio transmitter codenamed Q58 outside London coordinated all the different radio signals being sent during a particular bomber mission, working on all the different frequencies being used from the home air base of the bomber and fighter support squadrons, the air sea rescue service in the Channel, night-fighter support units and British radar installations. The longer the bombers' route to the target was and the more aircraft involved, the more signals were generated, and the more material the Germans had to work on. If a mission was cancelled or postponed, a signal was then sent to every single unit involved in the mission, every time using the word 'cancelled' or 'postponed', thus giving German cryptanalysts a repeated one-word crib into the RAF's Bomber Code, however often it changed. Not all RAF units, however, gave away information about their operations or deployments. Ludwig estimated that the two outstanding examples of RAF radio discipline were the 5th Bomber Group, which included the 'Dambusters' of 617 Squadron, and 138 Squadron based at RAF Tempsford, which flew Allied agents in and out of occupied territory. These two units' radio discipline was such that their flights often took the Germans unaware. Ludwig's unit spent their days and nights listening in to the tell-tale signature call-signs of Spitfires, Hurricanes, Wellingtons, Lancasters, Halifaxes and Mosquitoes operating all over southern England. He knew their call-signs so well that he and his unit had built up an operational order of battle for many of the USAAF and RAF squadrons based across the Channel in front of him. He was under no misapprehension that the British had triangulated his radar beams and signals transmitters. The British Parachute Regiment and a group of air force technicians had 'pinched' enough sensitive Freya and Würzburg radar equipment from an airborne operation against a radar station at Bruneval on the northern French coast in

1942 not to know what German units like Ludwig's were doing.

Operation *Jubilee*, when it came, was a complete disaster. The Germans on the northern Atlantic coast of France had been following the radio transmissions of RAF squadrons all over England, and so were aware that at a future given moment, an amphibious assault was coming somewhere between Cherbourg and Calais. They did not know where or when, but every German unit on the coast was constantly put on high alert, and at key possible assault locations, such as Dieppe, machine-gun and artillery companies had practised zeroing in on stretches of beach that could be used for landings.

The RAF flew over Dieppe and Harfleur and the rest of Normandy on most days, looking for German fighters, or en route to bombing missions in France or eastern Germany. So when, in July and August 1942, Ludwig picked up repeated call-signs of RAF squadrons massing in southern England, he knew something was up, but not what or when. Contrary to what the British would claim after the raid, the Germans had no forewarning of the Dieppe landings. Ludwig was adamant about this. The approach of the assault force off the coast was not picked up by radio interception units or cryptographers, mainly due to strictly imposed radio silence. Yet the wireless traffic at the beginning of the attack was, immediately, as soon as the Allied units arrived off the target beaches. Straightaway, Ludwig's men started listening to the wireless links between the headquarters ships in the Channel and their base in Portsmouth, signals between headquarters ships and units ashore, RAF and Royal Navy traffic, and the sea rescue service. Once the attacking force was ashore, many signals messages were sent in plain language, as the Allies thought, erroneously, that the Germans would not have time to read them before taking defensive action.

When the Canadians arrived on the Dieppe beaches, without naval gunfire support, it was a massacre, and many men did not make it off the beach in an attack that lasted six hours. A total of 60 per cent of the assault force were killed, wounded or taken prisoner, and the RAF lost 111 aircraft and seventy-three fighter pilots to the Germans' forty-eight aircraft destroyed, twenty-four damaged, thirty-four pilots killed and seven wounded. Six RAF squadrons flew the new Spitfire Mark IX, which was the only British fighter that could match the Focke-Wulf Fw190, but many Spitfire squadrons were operating at the extent of their range and could only spend five minutes over the target area.[1]

The commandos who aimed to steal the naval Enigma machine didn't

make it out of their landing craft, and tanks got bogged down in the shingle. Back in England, British Chief of Combined Operations Louis Mountbatten at first tried to present a fictitious propaganda picture of the attack, and then as word seeped out from the Canadian soldiers as to what had actually happened, London blamed intelligence leaks within the ranks of the French resistance. The German signals intelligence units around Dieppe stressed repeatedly in their post-operational reports that they hadn't known the Allies were coming until they arrived off the beaches – at which point their defensive preparations had swung into action.

The raid on Dieppe marked one of the lowest points for Britain in World War II. The Germans were delighted with the operational behaviour of their units around the town. The signals intelligence units came in for much praise, and Hermann Göring even mentioned their successes in a public speech, which had the unforeseen effect of making the Allies camouflage their land and air exercises in England after Operation *Jubilee*. Adolf Hitler decided to reward the town of Dieppe for not having helped the Allied assault, and so he freed from German custody French POWs who before the war were either from the town or had lived in it. On 12 September 1942, a train carrying approximately 1,500 French prisoners arrived at Dieppe station, and as a reward for what Hitler described as the 'perfect discipline and calm' of the town's residents, he gave the town a gift of ten million francs, to be used to repair the damage caused during the failed assault.[2]

Chapter Eighteen

U-91 AND THE BATTLE OF THE ATLANTIC

By mid-1942, the Allies estimated they needed more than a million tons of imported supplies per week to be able to sustain their war effort, and to ensure the survival of Great Britain. To make certain that this required tonnage of arms, fuel, food, medical supplies, aircraft and raw material arrived in British ports, in 1940 the Royal Navy had, of course, implemented a convoy system. Heavily laden merchantmen and tankers crossing the Atlantic were escorted by British, American and Canadian naval vessels. The convoy system had a primary flaw and a primary benefit for both the Allies and the Germans. Defenceless merchant ships gathered together were easier to protect with naval escort vessels. But for German submarines, the large groups of ships were easy to find in the vast waters of the Atlantic. However, this also made it easier, in turn, for the Allied naval vessels to find the U-boats.

Winston Churchill said that the Battle of the Atlantic was 'the dominating factor all through the war. Never for one moment could we forget that everything happening elsewhere, on land, at sea or in the air depended ultimately on its outcome.' [1]

The Germans' primary submarine strategy from 1941 onwards had been to adopt the *Rudeltaktik*, or 'pack tactic'. Britain depended on overseas supplies from its empire, and from the United States, Canada and South American countries. Throttling its maritime supply lines was vital. By mid-1942, the Germans knew that American trans-Atlantic troop convoys were also

transporting thousands of men to fight in North Africa. They were also aware that the Allies depended completely on the convoy system to be able to build up enough men and supplies in Britain to allow them to launch an invasion of mainland Europe. Finding, attacking, and sinking Allied convoys was thus clearly vital. The Rudeltaktik, which became known as the 'wolfpack tactic', was based upon groups of U-boats being guided towards the projected course of a convoy. The U-boats would then attack as a group; Allied escort ships would break away from the convoy to try to find the submarines, leaving the merchant ships unprotected. Finding the convoys in the thousands of square miles of the Atlantic was the primary challenge the U-boats faced in waging an effective, aggressive blockade of Allied merchant shipping. The Germans had only a small number of long-range Focke-Wulf Condor aircraft, based at Bordeaux and Stavanger, that they could use for airborne reconnaissance. Their primary and most effective source of information on the convoys' locations came from the breaking and reading of Allied naval and merchant marine signals.

By mid-1942, Wilhelm Tranow and his colleagues in the headquarters in Berlin were receiving hundreds of intercepted messages per week sent in from listening stations in France, Holland, Belgium and Spain, concentrating solely on Allied naval and merchant shipping movements across the Atlantic. German weather ships added further intercepted signals. Because they could now read both the Royal Navy's Cypher No. 2, and the British and Allied Merchant Ships Code, the B-Dienst's decrypters often knew the movements of both west- and eastbound Atlantic convoys before they even set sail. From their headquarters the information from the decrypted messages was then re-encrypted and sent to the U-boat service headquarters in Berlin and Kiel. The messages were then sent on to western France, to the submarine bases at Brest, Lorient and La Pallice, the deep-water port of La Rochelle. From there, they were encrypted using Enigma, and transmitted outwards towards the waiting U-boats in the huge, wide Atlantic.

One of the German submarine officers who received them was called Heinz Walkerling. Aged twenty-seven in 1942, he had joined the Kriegsmarine in 1935.[2] At the outbreak of war, he served first on a minelayer and afterwards on a destroyer for fourteen months. He then volunteered for a transfer, to serve in the high-risk, glamorous but highly dangerous submarine service. His U-boat training lasted six months, from October 1940 to March 1941, just after the period in 1940 when German submarines sank so much

merchant shipping that U-boat crews referred to it as 'The Happy Time', or '*Die Glückliche Zeit*'. Morale among German submariners was thus high when Walkerling joined his first boat, U-431, as a watch officer. He went on two patrols, before taking command of his own submarine in January 1942. U-91 was a brand-new Mark VIIC submarine, weighing 760 tons, and was 220 feet long, and fifteen-and-a-half wide. It had four bow torpedo tubes, one in the stern, and a range of 8,500 miles.

If the B-Dienst decrypters in Berlin were part of the technical brain of the German efforts in the Battle of the Atlantic, then Walkerling was at the tip of the operational spear. U-91 sailed from Kiel on 15 August 1942, as part of a wolfpack codenamed *Vorwärts* (Forwards), and attacked several convoys in the Atlantic. The pitch dark of the night of 8 September found it sailing on the surface, about 500 miles east of St John's, Newfoundland. The German U-boat headquarters had received information from the B-Dienst that a convoy codenamed ON127 was approaching the position of U-91 and the other submarines, and had signalled them to this effect. Walkerling and his officers already knew that the B-Dienst intelligence officers in Berlin and Brest were able to intercept and read coded signals sent by merchant ships in convoys, and their escorts from the British, American and Canadian navies. '*Group Vorwärts is ordered to take up positions in patrol line from AK 6664 to AL 7854 … The next convoy is expected about 9 September*,' said U-boat headquarters on 8 September.

By the 9th, they were proved correct. '*U-584 … sighted convoy of 11–15 steamers in AL 7463 at 2029 [Central European Time]. It was ON 127, which was expected at this time by dead reckoning.*'[3]

Heinz Walkerling and U-91 were part of the reception committee waiting for convoy ON-127.[4] At 6pm on 13 September, looking through his binoculars, he spotted a convoy in the gathering darkness, silhouetted against the sky.[5] The convoy, in staggered formation, was making a wide turn towards the north, and U-91 then lost them. So Walkerling ordered his helmsman to steer a southerly course since he expected the convoy to turn back onto a direct westbound heading. He was proved right. By 11pm, he found himself ahead of it, with a number of ships' silhouettes visible through his periscope. One of them was a twin-funnelled destroyer, moving at a slow speed. At 11.03pm,[6] sailing on the surface, he launched two torpedoes:

> A salvo of two torpedoes against the destroyer from tubes I and III. Target speed 11 knots, range 10 hundred metres … after 1 min 50 sees two detonations. Black-white detonation cloud and bright red flames. The destroyer lies dead in the water, burning fiercely.[7]

The destroyer in question was a Canadian ship, HMCS *Ottawa*, which, at the moment Walkerling attacked, was steaming westwards towards Newfoundland on escort duties for convoy ON-127. On its bridge was a Canadian officer, Lieutenant T.C. Pullen. He knew U-boats were waiting, and he had been told that the German navy was able to read Royal Navy signals by that stage of the war:

> The enemy was routinely reading our signal traffic. In the case of ON127, BdU (Befehlshaber der U-boote, or Commander-in-Chief, U-boats), already aware of our existence, was wasting no time in laying on a reception committee.

But on board *Ottawa* that night, he was taken completely by surprise by the torpedoes:

> Then, out of the night, a tremendous clap of thunder from forward, the stunning blast of an exploding warhead. The ship's forward superstructure, funnels, bridge, all that part visible from where I stood agape, became momentarily silhouetted by an orange glow, followed by darkness and an ominous silence … immediately afterwards, the stokers' living quarters was framed by torn and twisted steel. Underneath the wreckage could be heard groans from a few victims who had survived the blast and were in great distress. Above me were the bloody remains of lifeless men smashed upwards from their hammocks and impaled on overhead fittings by the tremendous force of the explosion. In the light of my torch the battered face, or what remained of it, of one familiar stoker was barely recognizable.*

Shortly afterwards the *Ottawa* turned almost vertical, bow first, and sank. A total of 137 men died, while forty-five made it into lifeboats or onto floats, and were rescued. Pullen and the remaining crew made it back to Canada, and in the immediate aftermath of the sinking, there was a Board of Inquiry. Although the investigation focused on the lack of radar being fitted to old

Canadian destroyers like *Ottawa*, there were subsidiary findings. Pullen was told in writing afterwards by a British convoy escort leader, Commander Peter Gretton, that British operational command for Western Approaches, at Derby House in Liverpool, had known that the German navy had been able to read all of the signals sent by both merchantmen and escorts of convoy ON-127.[†]

In the meantime, Walkerling and the crew of U-91 had arrived safely back in Brest on 6 October 1942.

The Greatest Convoy Battle of All Time

By March 1943, Walkerling's submarine, or *U-Boot*, was operational once again. In the middle of that month, it was on its third Atlantic patrol, 300 miles due south from the tip of Greenland. His boat was part of one of three wolfpacks that were stretched out in two lines. The account of the number of U-boats in the wolfpacks or sailing nearby, or deployed independently, varies slightly, but officially there were forty-two submarines in all three packs.[8] They were divided into three groups, codenamed *Raubgraf*, *Dränger* and *Stürmer* (Robber Baron, Daredevil and Harrier). It was one of the largest concentrations of U-boats deployed on a single operation in the whole of the Battle of the Atlantic, which by that freezing spring of 1943 was entering its fourth year. The Germans could see the invasion of Europe coming, and were determined to do their utmost to cut off the convoy routes. As such, the month of February 1943 had shown an increase in U-boat concentrations in the North Atlantic. Admiral Karl Dönitz now had 212 U-boats under his command. A hundred of them were at sea at any one time. The tonnage of Allied shipping being sunk was at its height, despite the British cracking of the Enigma coding system.

The German U-boats knew that their best hunting grounds lay in a crucial part of the North Atlantic. The limited range of British B-24 Liberators, Sunderland Flying Boats and American B-17 Flying Fortresses based in Newfoundland, Iceland and Northern Ireland meant that a so-called 'air gap' existed in the mid-Atlantic. The U-boats preferred to attack at night, often on the surface, which allowed them greater speed, visibility and manoeuvrability. The long North Atlantic nights hid them from patrolling ships and aircraft. And in the air-gap attack conditions were at their best, as there were no aircraft at all. Some Allied ships called the air gap the 'black pit'.

The wolfpack codenamed *Raubgraf* comprised thirteen U-boats, *Dränger* eleven, and *Stürmer* eighteen. Another four boats were sailing independently nearby, and several submarines from the wolfpack had also broken off from the group after a previous attack on a convoy. The weather off the southernmost tip of Greenland in that second week of March was unspeakable. Gale-force winds pulled barrages of sea fog and mist across the fifteen-foot-high freezing waves. The conflicting currents that swirled around Greenland and Newfoundland hit each other in a boiling meeting point. Visibility was low, there was near-constant freezing rain, and low cloud cover. These were the worst possible conditions for large, slow, heavily laden merchant convoys to be crossing the Atlantic. But at the same time, the foul weather also made it much harder for the U-boats. When they fired a torpedo, the submarine commanders needed their boat to be as stable as possible, otherwise aiming was a problem. With fifteen-foot waves and swirling currents tossing the U-boat around, it was extremely hard to keep a steady aiming point on a merchant ship in the dark. At 12.14pm on 14 March, the *Raubgraf* pack received orders from their headquarters in Lorient, on the Atlantic coast of France. They were to divert at high speed south-west towards Newfoundland, to form a new attack line, and wait for a convoy. So immediately they turned to change position, and headed south-west on the surface. The Mark VIIC boats in the group could make seventeen knots, or twenty miles per hour, on top of the storm-churned waves, but only half that submerged. The lookouts posted on top of the conning towers were soaked to the skin in freezing seawater. They'd been underway for exactly six hours and forty-seven minutes when another radio signal arrived, contradicting the previous one. Return to your former positions south of Greenland. Immediately. Thirty-seven minutes later came another instruction: 'Lock onto incoming eastbound convoy.'

At 8pm that evening, one of the submarines in the *Raubgraf* pack surfaced like a storming whale bounced upwards from the depths. It was U-91, commanded by Heinz Walkerling. After more than a month at sea, much of it underwater, the captain and the fifty-odd members of its crew were exhausted.[9] Their uniforms were covered in mildew and stained with engine oil, while the men themselves were unshaven, white-skinned and filthy. They were living in an enclosed metal tube, every man's limbs bruised and cut from repeatedly thumping into the myriad metal fittings of the submarine's interior as the boat dived, changed course and plunged. The interior of U-91

stank, of diesel, unwashed feet, sweat, stale food, faeces and fear.

Living conditions on operational U-boats were appalling. Apart from cockroaches, noise, lack of space, lack of natural light and the all-pervading stench of diesel fuel, food was a constant issue. At the beginning of a patrol, the crew would fill the submarine with as many fresh provisions as possible. Although the U-boat crews received the best rations of any of the German armed services, the conditions in which they kept them and consumed them sometimes cancelled out this benefit. A total of 494 pounds of fresh and cooked meats, 917 pounds of fresh lemons, 595 pounds of fresh eggs, 408 pounds of marmalade and honey and 505 pounds of butter and margarine were just some of the supplies carried for fifty men on one particular three-month patrol. The problem, however, lay in preserving and storing the non-tinned food, which began to rot after ten days on a cramped U-boat with limited fresh oxygen. The submarines used any available space for storage, often filling one of the U-boat's two tiny cramped toilets, and its cubicle, full of food. The bread grew white coats of mildew, leading sailors to christen it 'Rabbit Bread'. Submarine captains often filled one of the ship's water tanks with diesel fuel, to extend its combat range.[10] Men estimated that they would spend three months never more than eighteen inches distance from another crewmember, and one U-boat captain remembers that on patrol he could recognize some of his men simply by the noise they made when brushing their teeth. Men washed in buckets of seawater and skin rashes and infections were common, partly as a result of the soapy scum that remained on the skin. They rinsed their dirty uniforms overboard, tying them in a roped bundle that was trailed from the hull when the ship surfaced. But despite all this, the morale of U-boat crews tended to be extremely high.

So just before 8pm on 14 March, U-91 came up to periscope depth, and then surfaced. Five men, including Walkerling, climbed up inside the conning tower, and clambered through the entry hatch. As they stood up, the full force of a North Atlantic gale hit them, and within minutes the waves crashing into the side of the boat had splashed violently upwards, soaking each man. Looking intently westwards with Zeiss binoculars into the low darkness, Walkerling saw a series of string-like shapes that linked grey scudding sea and black, racing sky. Smoke trails. It was a convoy. Back in France, the U-boat headquarters had been working perfectly in tandem with the B-Dienst in Germany, meaning that out in the waters of the Atlantic, submarines like U-91 were guided perfectly onto their targets.

Suddenly, without warning, three American aircraft appeared from the dark clouds above the U-boat. This was every submariner's nightmare: to be caught in the open, on the surface, by aircraft loaded with depth charges and bombs. The five men ran for the hatch on the top of the conning tower, while one man screamed the news down the voice-pipe to the submarine control-room. Walkerling ordered the crew to crash-dive, and as the boat plummeted down into the Atlantic, the dark waters swirled past the white horse emblem on the U-boat's conning tower. Walkerling was guessing how the aircraft had found him. He knew that in between receiving the three conflicting sets of radio instructions that same afternoon, five of the U-boats in the *Raubgraf* pack had transmitted responses: two had reported their exact positions, and three had signalled the presence of Allied aircraft overhead. Allied ships, fearing the presence of U-boats in the area, had obviously alerted aircraft equipped with direction-finding radar, which had pinpointed his position. There couldn't be any other explanation, he thought. And shortly, his U-boat was deep enough to be out of danger from the aircraft's depth charges. So as his submarine levelled out of its crash-dive, Walkerling turned to his signals officer. '*Geleitzug! Standort sofort melden.*' Convoy. Report position at once.

U-91 sent and received radio messages on the Naval M4 Enigma machine, using any one of some fourteen different code settings. Since February 1942, Walkerling and other U-boats in the Atlantic had used the cipher codenamed 'Triton', which the British called 'Shark'. To transmit messages about convoy sightings, the radio operators and signals lieutenants on board U-boats took their daily cue from the *Kurzsignalheft*, or Short Signal Book. The operator took the daily Enigma 'key' for whichever cipher he was using, and set the rotors, plug, switchboard and ground settings of the machine accordingly, before encrypting messages. The first word of outgoing or incoming messages from and to submarines was either *Allegemein*, or 'general', or *Offizier*, meaning 'for officers only'. These latter messages were doubly encrypted. To read them, the U-boat's radio operator set his Enigma machine to that day's settings, and decrypted the message. It was then passed to the signals lieutenant, who would re-format the Enigma machine to another pre-specified setting only the officers knew. Once read in plain script, it went to the captain.

Walkerling had confidence in his superiors' judgement whenever they sent him a seemingly contradictory radio instruction. As had just happened thrice

that same afternoon south of Greenland. Walkerling and most of his fellow U-boat captains had worked out that his colleagues in German naval intelligence had to be reading some, if not all, of the Allies' naval codes. How else to explain such precise instructions as he had received that afternoon? Walkerling's superior officers were always saying to him and to his colleagues that the Enigma enciphering machine was utterly secure. It couldn't be broken, they said, and although there had been occasions during the war so far when they suspected the system might be compromised, subsequent investigations proved it hadn't. It gave the U-boat commanders huge confidence to know this, as they set out on their patrols into the Atlantic.

Walkerling also knew the Enigma settings themselves were always being changed. Just five days before, on 10 March, some of the key codes had been changed once again. He had received instructions on that day to change his Short Weather Code book, his *Wetterkurzschlüssel*, to an updated version, the Mark III. So now, whenever his boat transmitted a weather report – and this happened frequently – the cipher and the daily key used to set the Enigma machines were completely different to anything that had preceded this. And now, out in the North Atlantic in March 1943, he could see that the Germans knew which convoy was heading where, when, and at what speed. The Germans could see everything. And what was now approaching across the storm-crashed waves of the North Atlantic, coming towards Heinz Walkerling and the other forty-one U-boats, was big. Very big.

The Convoys

The U-boats were positioned on the western edge of the 'air gap', south of Greenland, with *Raubgraf*, *Dränger* and *Stürmer* deployed in a roughly vertical line from north to south. A strong North Atlantic storm blew up on 14 March, making the already desperate weather conditions worse. But the convoys welcomed bad weather, as although it made sailing conditions deplorable, and life on board ship beyond miserable, the U-boats found it much harder to operate. One of the submarines in the *Raubgraf* group, U-653, then found itself low on fuel, and as it only had one defective torpedo remaining, headquarters instructed it to return to Brest. As the storm thickened on the 15th, it headed south-east into the mid-Atlantic. Surfacing briefly, its crew found the storm so strong that a watch party stationed on the conning tower were swept overboard into the waves; luckily they were

attached by safety ropes. The submarine pushed forward, its crew catapulted around in the hull by the force of the storm. Suddenly large, grey shapes appeared in its periscope, rising and falling on the waves and in the vast sheets of rain. It was a convoy. The U-boat sent a two-word radio burst, along with position coordinates. Convoy sighted. Heading due east. The wolfpacks gathered for the attack.

HX-229 was a convoy of forty-three merchant ships that had left New York on 8 March, bound for Liverpool.[11] Its escort consisted of Escort Group B-4, made up of a group of five destroyers, HMS *Volunteer*, *Beverly*, *Witherington*, *Highlander* and *Mansfield*, and three corvettes, HMS *Anemone* and *Pennywort*, and the Canadian vessel HMCS *Sherbrooke*. Nine other British, Canadian and American escort vessels accompanied the convoy at various stages across the Atlantic, in some cases joining it on arrival in Iceland; the *Witherington* was with the convoy only for one day, as it suffered weather damage. On paper this looked an impressive number of escorts, but in reality it was slim protection for such a large convoy in such appalling conditions, and the number of U-boats almost matched the number of ships in the convoy. *Stürmer* and *Dränger* attacked from ahead of the convoy, *Raubgraf* from behind. Twenty-seven merchant seamen drowned or were burned to death when the American freighter *Walter Q. Gresham* took a torpedo that blew off its stern. Forty-two survivors were pulled out of the sea, from a frothing mass of seawater mixed with hundreds of tons of powdered milk and sugar, the cargo it was carrying. The *Canadian Star* was hit and went to the bottom, carrying its cargo of meat, butter and cheese. Twenty-nine of the ship's crew of eighty-three burned and drowned, left face down in the waves in lifejackets. The *Southern Princess* was carrying a vital convoy of aviation fuel, railway locomotives and precious landing craft needed for amphibious assault operations. One torpedo filled its hold with seawater, and the weight of the shifting cargo capsized the ship.

In the early hours of the 17th, U-91, under Heinz Walkerling, attacked the American freighter *Harry Luckenbach*, loaded down with nearly 8,400 tons of cargo. In the space of four minutes, between 3.37am and 3.41am, the U-boat launched five '*aale*', or 'eels', as the German submariners called their torpedoes. They hit the freighter amidships, straight in the engine room. It went down quickly, although the seventy-nine-man crew managed to take to the lifeboats, and were all alive when they went into the water. The corvette HMS *Pennywort* came to their rescue, but was so burdened by 108 survivors

from other ships that it left the crew of the *Luckenbach* to other escort vessels. By the time HMS *Anemone* broke off from tracking U-boats to pick up the crew, their three lifeboats had disappeared. It was pitch dark, in an Atlantic storm, 400 miles south-south-east of Greenland, in winter. The men were never seen again.

U-91 fired three more torpedoes at two freighters, the *Nariva*, carrying meat, and the *Irénée du Pont*, carrying nine aircraft. The first was crippled, the latter sank. Three more ships in the convoy were damaged, and only one U-boat was lost. There was no 'rescue ship' sailing with HX-229, the vessel whose duty it was to trail behind the convoy and pick up survivors. So three of the convoy's escorts assumed this job, leaving only two destroyers or corvettes to hunt the massed U-boats. By the time Liberator aircraft flying from Iceland and Northern Ireland arrived over the convoy late on the 17th, the battle was done, the U-boats withdrawing back to France. It was a massacre. Eight ships were torpedoed during the night of the 16th alone, and the battle continued for the next forty-eight hours. The list of ships sunk, and the cargoes they were carrying, was the story of the Battle of the Atlantic, and the desperately needed supplies they were carrying to Britain. Steel, cotton, aircraft, manganese, zinc, steel, grain, trucks and thousands and thousands of gallons of aviation fuel were among the cargoes that were sunk. Heinz Walkerling and U-91 accounted for three of the thirteen ships that went to the bottom.

Simultaneously, other U-boats had joined in the attack on another convoy, SC-122, following behind HX-229. This was even larger, containing sixty-five ships, and had a central escort group of two destroyers, a frigate and five corvettes, while another ten vessels escorted part of the way outwards from the American coast, and from Iceland back to Britain. U-boats from both *Stürmer* and *Dränger* attacked it: nine merchantmen were lost. The Germans were to describe the attacks on HX-229 and SC-122 as 'the greatest convoy battle of all time'.[12]

The Signals Compromise

Hardly had the convoys been attacked than both the British and American navies started carrying out a damage assessment operation.[13] The first question was simple. How had three large U-boat packs been in exactly the right place, at the right time, to ambush two large convoys? How had they

managed to adapt their positions to the movements of the two eastbound convoys, no fewer than three times in the days and hours leading up to the attacks? The British codebreakers at Bletchley Park had not been able to provide decrypts of the U-boats' location signals or weather reports during the period from 10–19 March. They had previously used the Germans' Short Weather Code book, Marks I and II, as a 'crib' to break into messages enciphered on Enigma. But when this book was updated on 10 March, for the crucial period during the convoy battle, the Allies were operating 'blind'. The changes and updates to the Enigma codes had meant that an extraordinary stroke of operational luck they had in autumn 1942 was now outdated. On 30 October 1942 the submarine U-559 was sunk with depth charges off Port Said in the Mediterranean; but not before three British sailors from the destroyer HMS *Petard*, two of whom drowned, had managed to rescue the submarine's Enigma key setting sheets, with all the current settings for the German naval Enigma. However, five months later, once the Allied signals analysts had managed to break back into the newly changed 'Shark' weather code by 21 March, back-decrypts of messages sent before and during the convoy battle south of Greenland showed clearly what had been happening. The Germans were reacting in almost real time to a variety of signals sent by the merchant ships, by their Royal Navy escorts, by the Allied Headquarters for the Western Approaches, based in Liverpool, and by the Americans. It was frighteningly clear that they were reading some, if not all of the Allied naval codes.

The Germans, as previously described, had managed to achieve this through a variety of methods, and because of a number of external factors. In 1941 the United States Navy, under its commander-in-chief, Fleet Admiral Ernest King, had refused for security reasons to equip any British naval vessel with their ECM Mark 1 encryption devices. Consequently, the British Admiralty decided it was time to upgrade their own enciphering technology, and by 1941 they had introduced Naval Cypher No. 2, and then latterly No. 3 for all signals transmissions in the whole of the Atlantic, essentially from the northern Arctic Circle down to the Antarctic, which would now operate in conjunction with other administrative and merchant navy codes as well.

But hardly had the hulls of the sunken freighters from convoys HX-229 and SC-122 touched the bottom of the deep Atlantic, than further proof emerged that the Germans were indeed reading British coded signals. Three thousand miles to the south of Greenland, and the site of Heinz Walkerling's

battle in U-91, lay much warmer waters. On 18 March 1943 German U-boats lying off the Caribbean island of Trinidad received an '*Offizier*' message. A convoy, codenamed TO-2, would be arriving in Trinidad on 21 March. The message was very specific: the convoy's exact route was given, along with three coordinates along its journey, its estimated time of arrival, and its escort strength. There were even comments made by the Royal Navy's Operational Intelligence Centre, or OIC, in Gibraltar as to the likelihood of the convoy being attacked.

The codebreakers at Hut 8 at Bletchley were trying to find out what had happened with the German penetration of the Royal Navy's codes. By 25 March they were reading 'Shark' again; this was the key to Enigma material based on decrypts of the new Mark III version of the U-boats' Short Weather Code book. They saw what was happening by the beginning of April 1943. They backtracked through signals sent by the British Royal Navy's OIC in Gibraltar, and there it was. At 10.42pm on 10 March – when Bletchley Park had been 'blind' to 'Shark' – a signal had been sent from Gibraltar to the American convoy escort destroyers USS *Decatur* and *Roper*. It was encoded in Royal Naval Cypher No. 3, with daily subtractor codes based upon the Royal Navy's Reference Table S. The Germans had read it. Both the British at Bletchley and the Americans in Washington and at Norfolk Naval Base in Virginia realized that this German deciphering of their codes could be the rule, not the exception. Both went backwards through their signals to the beginning of 1943, looking for what might have happened.

While they were doing this in the first week of May, two convoys codenamed HX-237 and SC-129 were forming up to leave New York and Newfoundland. Enigma intercepts and decrypts from U-boat position reports and weather transmissions showed very clearly that two wolfpacks, codenamed *Rhein* and *Elbe*, were waiting for them. They were in a long vertical line off Flemish Cap. This was an area of shallow water some 350 miles due east of Newfoundland. The convoys, their escorts, and shore bases in America and Canada were in touch constantly, all using the same Naval Cypher No. 3, using Substitution Table S. So the German decrypters at the B-Dienst had plenty of signals material to go on while the convoys formed up. There was a lot of fog, and the ships were being marshalled very carefully, and so a lot of signals were being sent. Because Enigma intercepts had alerted them to the U-boats' presence, Allied naval staff diverted the two convoys away from the presumed *Rhein–Elbe* patrol line. But shortly afterwards, the

U-boats themselves also received the Allied messages, broken by their own naval signals analysts back in Berlin, and simply shifted position accordingly.

Bletchley Park also had plenty of material to work with, as the U-boats had a habit of using the same three words to advise of a convoy's approach. '*Ein erwarteter Geleitzug*': an approaching, or expected convoy. Hut 8 continued to use this as their crib, and more of the U-boats' secrets then came out. On 6 May, at 9.30pm, the British and Americans had signalled the exact location of the two convoys leaving Newfoundland and New York. This was given as 45 degrees 56 north, 48 degrees 27 west. Just two hours later, by 11.30pm, the Germans in Brest – who had no possible visual sightings of the convoys – were transmitting the same coordinates back to their U-boats waiting off Flemish Cap. With tiny errors: 45 57 north, 48 25 west. The Naval Cypher No. 3 was clearly blown wide open.

Within days it became apparent to the British that these three incidents were no mistake. Between January and June 1943 they established thirty-nine separate examples where Naval Cypher No. 3, with Substitution Table S, was compromised in real time.

There was enormous concern about what had happened to convoys such as HX-229 and SC-122, but the Allies believed that their exposure only extended as far back as November 1942. They were wrong. Because they were about to discover that the Germans had been reading British naval codes for a substantial period before that. Long before 1942, and 1941. For Wilhelm Tranow and the Germans had of course first begun cracking the British Royal Navy's ciphers in 1935.

Another U-boat action, very similar to the one involving U-91 and Heinz Walkerling, took place in February 1943, when the U-boat packs *Neptun*, *Ritter* and *Knappen* (Neptune, Knight and Squire), involving a total of twenty-eight submarines in all, were on station in the Greenland Gap. Dönitz had formed these three wolfpacks into a patrol line on the meridian of 30 degrees west, beginning in 63 degrees north and stretching southwards for 600 miles to 53 degrees north. In February 1943, there was a successful attack on convoy ON-166, and the Admiralty suspected that Naval Cypher No. 3 was compromised, although at that point they had not carried out the in-depth investigation that could prove it. Last-minute shifts in the patrol lines of groups *Ritter* and *Neptun* on 18 February showed that German U-boat headquarters had abandoned the plan of conducting operations on convoy HX-226 but was instead reforming attack group lines to target the westbound

convoy ON-166. Within a few moments of these changes, a third group of U-boats was formed to swing out to the south-east of the *Neptun–Ritter* line and cut off any southerly diversion of the convoy.

U-boat U-604's hydrophone made contact with the convoy's propellors. Convoy ON-166 had received three diversions by 18 February 1943, sent by the Admiralty using Naval Cypher No. 3, reciphered using Table S, and so it had attempted to proceed south. That Wilhelm Tranow had known about the convoy was unquestioned in the Admiralty.

The disposition and shifting of the U-boats in the last ten days of February suggested that the B-Dienst had knowledge of the location of the convoy rather than a reckoning. The first of the three diversions was the most suspicious, as it would have sent the convoy bang through the middle of the *Ritter* line, with other ships diverted straight at the *Knappen* group of U-boats. On 26 February 1943, the Atlantic section of the Admiralty sent a message to the commander-in-chief of the US Fleet (COMINCH) commenting on the strange and inexplicable behaviour of the wolfpacks during these operations. Further evidence had accumulated after the battle of convoys HX-229 and SC-122, which the British, and not just the Germans, considered the largest U-boat battle of World War II, at a time when B-Dienst solutions to 'Frankfurt' were at their peak of efficiency.

The two convoys that had been attacked in mid-March were HX-229, which had left New York City on 8 March, and a slower convoy, SC-122, which had left New York City on 5 March. The faster HX-229 had overtaken the slower convoy by the time the U-boats attacked.

On the 12th and 13th, SC-122's sixty-five vessels steamed in thirteen columns, while HX-229, which was catching up on SC-122, was steaming in eleven columns, both heading for the North Atlantic, when the Admiralty heard heavy U-boat communications ahead of the two convoys. At 8pm on 13 March SC-122, currently at 49 degrees north, 40 degrees east, was ordered to avoid the U-boats, by steering a course of 67 degrees. B-Dienst decrypted this message, and passed it to Karl Dönitz.

The U-boat wolfpacks then adjusted their position. It would be difficult to account for *Raubgraf*'s sudden shift, as the Royal Navy later said with magisterial understatement, without assuming compromise. The Royal Navy attributed the insecurity of Naval Cypher No. 3 to three main factors: the same codebook had been used for too long, giving the Germans large amounts of 'depth' which they could use to decipher it; even though the

Substitution Table 'S,' and another one called 'M' were changed every ten days, overuse of them gave the Germans repeated cribs and depth; the distinctive call-signs used by the Royal Navy made it easy to identify and intercept their signals. So on 1 June 1943 Naval Cypher No. 5 was introduced, and while the British were taking decisive precautions – albeit late – the Germans still remained unaware that for over three years the British had been reading their messages enciphered in Enigma codes.

---

* Before he died in August 1990, the last thing retired Captain Pullen wrote was an account of the sinking of the *Ottawa*. It was published in the *Northern Mariner*, the journal of the Canadian Nautical Research Society. It appears in Volume 2, Number 2, on pages 1–27, in the article entitled 'Convoy ON 127 and The Loss of HMCS Ottawa, 13 September, 1942: A Personal Reminiscence'. His quotes about the attack on the Ottawa are all drawn from this.

† Gretton became one of the most highly decorated British naval officers of the war, being awarded three Distinguished Service Orders, a Distinguished Service Cross, Mentioned in Dispatches, and made a member of the military OBE. He was later made a Knight Commander of the Bath and became Deputy Chief of Naval Staff.

PART FOUR

GERMANY DEFENSIVE

Chapter Nineteen

THE BATTLE OF THE AEGEAN

From the radio intercept station that he had built north-west of Athens, Captain Ferdinand Feichtner woke up each day to the air of the Mediterranean. Hot sun in spring and summer, dusk plunging fast and gold into the cobalt blue of the Aegean that lay on the horizon to the west and south, and then cold snaps of winter wind. His life seemed to be inextricably mixed with the air above and around him: each day he and his men scanned the radio frequencies that the RAF used, flickering through the atmosphere. On his promontory he seemed to be closer to the sky than the land. The intercept equipment he had installed on the plateau north-west of the Greek capital was designed to listen to Allied air traffic over the eastern Mediterranean and North Africa area. It supported the Africa Corps fighting in North Africa, and could also pick up signals from as far away as Romania and the Russian border. He could sense the urgency and vast size of the fighting during Operation *Barbarossa* and its aftermath, via the signals that his station intercepted. It wasn't the job of his unit to monitor them, or to intercept them and pass them on for decryption and analysis, but he heard them anyway. There were signals from Army Group South as it closed in on Sevastopol, with a large amount of traffic in Romanian sent back to Bucharest by the units supporting the Wehrmacht. Curiously, there were Turkish police reports too, and diplomatic messages from Ankara. The country was still holding hard onto its neutrality, and Feichtner knew the British were using

the islands and coves along and off its shores to hide small special forces bases. He could hear the crackle of Italian naval signals as well, both from their ships in the Mediterranean chasing Allied supply convoys, and from messages sent from Rome to their naval units in the Black Sea.

After building his station, he had needed men to fill it, so he took a unit which had been based in the Balkans, doing little, and trained the soldiers to his own specific needs. He was fast acquiring a reputation within the Luftwaffe signals hierarchy as a man who got things done, an efficient and occasionally ruthless officer who had no truck with stupidity or inefficiency, but was also a commander who was fair on his men, while simultaneously demanding very high standards from them.

The original signals platoon he had brought with him from Asnières had, by early 1942, grown accustomed to his way of working, and he was constantly giving them new jobs. One of these was to intercept messages that were coming from a logistical radio network somewhere in Africa, across the Mediterranean from his Greek headquarters. It originated from a new supply net in central Africa. The messages contained information on all British aircraft movements from the cities of Sekondi-Takoradi and Accra in Ghana. These would travel to Khartoum in the Sudan, and thence onwards to Egypt. The signals were sometimes sent unenciphered if they appeared to the sender to be of low-level importance, but a message that specified arrival times or departure times from Ghana to Khartoum of 'cargo' could only refer to aircraft or supplies of spare parts.

The encrypted messages were in a four-figure variant of the RAF Code; the central decryption unit at Potsdam run by Dr Ferdinand Voegele would decipher them, and they gave information about each separate aircraft that was being transported across Africa: Hurricanes, Spitfires, P-40 Tomahawks and Kittyhawks, Beaufighters and C-47 Skytrain transport aircraft. These messages also helped the Germans work out the exact state of the airfields to which they were travelling, as requisitions for spare parts and materials needed for airfield maintenance went back down the same delivery line that brought the aircraft.

The signals gave an operational picture of the Allies air-readiness both on the front line in Egypt and Cyrenaica, but crucially behind the lines as well. Part of this information came from what were called the 'distribution groups' which, along with an indicator, began every message. Four-figure letter codes would be used to indicate that the message was destined for the RAF in

Khartoum, each front-line fighter base in Egypt, or RAF headquarters in Cairo, Haifa and Sierra Leone. This helped the Luftwaffe find out where the British air force was based, and the fact that the British only changed their distribution groups every six months was of even greater assistance. Although the groups changed in size and content, there were always the same central headquarters and airbases included in every distribution one – Khartoum and RAF staff headquarters in Cairo for example – so this provided reliable cribs into the four-figure code. Feichtner's job was then made even easier when the British changed the four-figure code in December 1941: they altered the code, but left the distribution groups the same. This meant that the Germans, knowing the old code for 'RAF HQ Khartoum' now had it repeated back to them in the new cipher.

The next task the reliable German captain set for his men was establishing another intercept station, this time on the island of Rhodes. He had also set up a new decryption office in Athens in the winter of 1941 where four-figure messages could be properly handled, away from the rudimentary conditions at the Loutsa plateau, which Feichtner still considered to be a 'summer house'. The Athens station was soon handling six to 700 messages a day, on everything from shipping movements, convoys, aircraft patrols, and the ebb and flow of German and Allied movements across North Africa. At the end of 1941, Feichtner was promoted, and made a major and regimental commander.

He sent one of his intercept platoons to North Africa in 1942, designed to try to replicate the success of 621 Company, but almost as soon as they arrived Rommel started retreating, and the men were brought back to Greece, and sent to a new headquarters on Mount Parnassus. This limestone mountain in central Greece towers over the plain surrounding it, and at 7,500 feet high, it provided the perfect location for a radio monitoring and intercept station. Within weeks of the establishment of the base, the Luftwaffe ordered Feichtner to send a team of four cryptanalysts to work with the Italian navy, the Regia Marina, in Rome.

This was a mixed blessing: on the one hand, Feichtner and his colleagues at the B-Dienst knew that the Italian navy under Admiral Donini had intercepted and read into a substantial number of British four-figure naval and merchant naval codes from convoys and their escorts in the Mediterranean. The Italians had kept very precise records of these codes and both the Luftwaffe and, particularly, the Kriegsmarine were extremely

interested to know if there was a cryptanalytical correlation between the results the Italians were achieving, and what the Germans were managing to read of British naval codes in the Battle of the Atlantic, which was then at its height and in its third year.

On the other hand, Feichtner did not trust the Italians, and suspected that if and when the Allies eventually invaded their country, they would capitulate. So he decided to cut his losses. And so he tried to confound any cooperation with them at any turn, and rather than take advantage of the opportunity to learn what British codes and messages they had or hadn't broken into and read, he decided to ignore the Italian offers of help. In return, he felt, this meant that he didn't have to reciprocate and show them how the German Luftwaffe was breaking four-figure RAF codes.

By summer 1942, Rommel and the British Eighth Army were alternately attacking and defending: the first battle of El Alamein in July had seen German and Italian forces advance to within sixty-five miles of Alexandria. Italian Bersaglieri troops marked this point, the furthest east they would advance in Egypt, with a commemorative stone. '*Manco il fortuna, non il valore*,' it read: 'Luck was lacking, not bravery.' The German and Italian supply lines from Tripoli were dangerously over-stretched, and it seemed Rommel had moved as far towards the Suez Canal as he could. Both sides waited for the expected British counter-attack.

While they waited, life was moving forward for Major Feichtner. His superior officer, General Wolfgang Martini, carried out an inspection tour of the Greek intercept positions. The combination of the arrival of his superior, whom he distrusted, the low morale of his men, and the residue of a long winter flu virus hit him all at once. In August 1942, he took his only leave of the entire war, and went home to see his wife Elisabeth in Germany. He tried to get the remains of Greek dust out of his respiratory system, and eat food that wasn't either tinned rations, or the opposite, the stomach-churning excesses of oranges, olives, lemons, melons and tomatoes which many German soldiers bought or bartered for in Greece. The benefits were that they were high in vitamins, and thus helped counteract the constant skin infections the men suffered from, a result of cutting themselves on sharp limestone rocks, and then trying, unsuccessfully, to keep wind-blown dust and the omnipresent flies out of the wound. The negative effect of the surfeit of fresh fruit was diarrhoea. So for Major Feichtner, three weeks of solid, steady and reliable German food from his wife was highly welcome.

In his absence an influx of untrained replacements arrived for the listening stations in Greece and at Taormina in Sicily. General Martini also sent two new commanding officers who knew little, if not nothing, of the signals intelligence procedures the Luftwaffe had worked so hard to establish, much of it under Feichtner's direction. Hardly, it seemed, had the Second Battle of El Alamein pushed Rommel's army reeling back from Egypt, than the Allied landings in French North Africa took place on 7 November 1942. Neither of the new senior officers had predicted this, and it seemed that changes, and new surprises, did not just stop with enormous and successful Allied offensives and amphibious landings.

In late autumn 1942, Feichtner's battalion received its first detachment of female auxiliaries to work both on the intercept station on the plateau at Loutsa, and in the Athens central evaluation station. Feichtner had seen this coming, and had indeed suggested that one way round the chronic staff shortages that ate away at his personnel rosters, with men constantly detached to Russia or Africa or France, was to use auxiliaries. And this largely meant women. The hard-bitten major of signals had argued several times with his superiors that if the German Post Office could use women to listen to telephone lines, monitor diplomatic communications, and even work on the A3 speech-scrambler system that listened to British and American trans-Atlantic conversations, then so could the Luftwaffe. Women, he said, were often far-better suited to radio work than men. They were calmer, more patient and methodical, and there were fewer disciplinary problems, too. His approach was that if a certain kind of person proved adept at listening to signals, then they should be employed to do so.

So with his female auxiliaries installed, the next step was to remove the two incompetent unit commanders from Athens and Taormina; as he was trying to lobby his blustering boss, General Martini, into making these changes, Feichtner knew it was time to concentrate on intercepting Very High Frequency messages from the RAF. Almost all of their units used VHF signals by late 1942, and up until then the Germans had found them impossible to pick up, especially at the huge distances they were covering, often in excess of 600 miles. So Feichtner sent a team of men to the coast of Crete to erect some aerials at different altitudes in different places, but with one constant caveat: the aerials should all face out to sea. In differing weather conditions, ranging from bright sunlight and calm seas, to storms, to days of heavy cloud cover, the men registered different results. Then, by designing his own type of

bipole antenna, Feichtner also increased the ability of his men to intercept VHF messages, meaning that the team on the Loutsa plateau could pick up signals from the Adriatic coast to the Crimea, including the Greek Aegean islands of the Dodecanese.

By May 1943, the Germans were expecting the Allies to invade the Italian mainland. Everybody expected them to begin in Sicily, but simultaneously British radio traffic started disseminating information that they knew the Germans would pick up, suggesting that the landings could come in Sardinia, Crete, on the coast of Yugoslavia, the Dodecanese islands or in Corsica. One way the Germans gathered information was by sending aircraft on reconnaissance missions over the North African coastline, looking for any signs of an invasion force being assembled. The missions were extremely dangerous: Allied fighters had recently shot down twenty-four of the Junkers Ju 52s and Ju 88s that made these flights. So Feichtner banned these hazardous missions, saying that they were a waste of valuable aircrew. After that, in conjunction with the German navy, he began to install a network of radar stations and radio intercept stations along the Adriatic coast of Albania, on Kos, Leros and Rhodes. The Germans, however, had yet another weapon in the armoury on whose door was stencilled the words 'Signals Intelligence and Cryptanalysis'.

The Germans Descramble the Trans-Atlantic Radiotelephone Link

Herbert Marinick was a radio expert from Berlin, born in 1902, who worked for the Deutsche Reichspost, the German Post Office.[1] From 1925 to 1932 he worked for Transoceanic Radio which maintained the radio links between the United States and Europe, and when this was taken over by the German Post Office in January 1932, he became the Telephone Inspector of the Reichspost. He continued working in this civilian capacity until he was attached to OKW-Chi from 1942 onwards. First in Holland and then in Germany, he and others worked on a device called the *X-Gerät*. This was a speech descrambler device that used two receivers to intercept traffic passed over the trans-Atlantic radiotelephone link between Washington and London. At the end of 1940 the Germans had realized that some unintelligible conversations were being heard on the trans-Atlantic circuit, which their Post Office was already listening to, as German industrial companies kept in regular contact with their subsidiaries in South America and Canada, even in

time of war. One of the transmitting and relay stations for this link was on the North Sea, in the Dutch town of Nordwyk.

Technicians from the Deutsche Reichspost and regular army signals intelligence technicians went to talk to the Dutch and listen to their records, and then built their own speech descrambler device. They took a frequency analyser and split the speech spectrum into twenty to twenty-five bands each of 100 cycles per second; the human voice varies in width between 100 and 8,000 cycles per second. In each individual link of the intercepted conversations the presence or absence of human speech was recorded, and so they made an optical analyser which meant that the frequency bands could be measured with a microscope. The analyser told them that the speech was being split into five bands, where the lower, middle and higher pitched sounds were individually recognizable. These bands were then inverted, which was the equivalent of a vinyl record on a turntable being played backwards. Once re-inverted, and the five bands reassembled, then human speech was decipherable. As this was in English, it then had to be translated, so the two lower frequency bands were mixed until audible conversation took place, after which the other three were added in. The incoming speech transmissions came via receivers, which were attached to the side of the device. It measured about six feet wide by four-and-a-half feet long and five feet high, and weighed 300 pounds. There was nothing revolutionary about the Germans' ability to work out how the device functioned: like much of their scientific work before and during World War II, it was based on existing research. The Dutch at Nordwyk who had worked for Siemens and Phillips in Eindhoven simply told the Germans where they could find an existing speech scrambler, which they then copied.

Their machine first became operational around the time of the invasion of Sicily in 1943. The staff of the Nordwyk station had moved to Ludwigsfelde on the southern outskirts of Berlin by this time, fearing raids by British commandos could steal their technology, as they had done at Bruneval in 1942. One staffer said he was told of a conversation between Churchill and Roosevelt which preceded the Sicily landings, and he said that this information enabled the Germans to withdraw back to the Straits of Messina, and thence back to the Italian mainland, with a lot of their equipment intact. Another man from OKW-Chi said that not only were conversations between Roosevelt and Churchill listened to, but also those of Queen Wilhelmina of the Netherlands talking in Dutch, and Winston Churchill talking to Lord

Halifax. During 1943 almost all the Allied conversations were in clear, while after August 1944 a codebook was introduced. At the end of 1943, the Ludwigsfelde station was destroyed by bombing, along with the speech scrambler, so the Germans simply decided to build another one, which would not be ready before summer 1944.

The Allies invaded Sicily in July 1943; by September they were ashore on the Italian mainland at Salerno. North Africa was lost, and the battle between Germany and the Allies was now focused on Italy. The Italians did exactly what Major Feichtner feared they would, and capitulated, agreeing an armistice with the Allies. Hitler, outraged but not surprised by the seeming duplicity of his former Allies, sent ten divisions of troops to reinforce Italy. These units streamed into the country from Yugoslavia, France, Austria and Germany. Mussolini fled, and Italian Carabinieri policemen, loyal to their king, briefly held him captive in a deserted resort hotel in the Apennines. German paratroopers and SS commandos then rescued him, and flew him to Berlin; the Führer allowed him to set up his own puppet fascist state in the north of Italy.

The consequences of this for Feichtner and for German troops in the eastern Mediterranean were immediate. General Eisenhower said that under no circumstances could the strategic situation in the Dodecanese islands, and across the eastern Mediterranean, be allowed to divert any resources at all from the fight for Italy, or influence the situation there in any way. This left islands like Kos and Leros still occupied by Italian troops. The Germans immediately rushed to take them over. Feichtner and his men were ordered to set up a chain of listening stations anywhere they could in the eastern Mediterranean, to help provide signals intelligence on any RAF flights that operated in support of British efforts to take these islands back from German control.

Operation *Tidal Wave*

Simultaneously, Luftwaffe headquarters in Berlin gave Feichtner another task they considered even more important. They wanted the Luftwaffe to install a radio-jamming screen that would protect the Romanian oil wells around Ploiesti from Allied air attack. The Third Reich was becoming increasingly dependent on Romanian oil, as the failure of Army Group South to reach the oil fields of the Caucasus meant that Germany's ability to find fuel for its

tank armies and aircraft was becoming increasingly stretched. By the end of 1942, 30 per cent of this fuel was coming from Romania. American bombers had made a failed attempt to destroy parts of the Ploiesti refineries in June 1942. The Germans had responded by increasing their anti-aircraft defences: they set up a protective chain of hundreds of flak guns, some of them hidden in railway cars, mocked-up buildings and even haystacks. Three Luftwaffe fighter groups were stationed around the area, and Feichtner's chain of radio intercept stations covered every angle of approach to the target.

Then in August 1943, the Allies tried again. Operation *Tidal Wave* saw five separate American bomber groups take off from airfields in North Africa, and fly towards Romania straight through the interception, radio monitoring and radar network controlled by the Luftwaffe's signals units. They flew over the Mediterranean and the Adriatic, thundered over Corfu and Albania, sliced across Yugoslavia, and entered Romanian air space. En route, Major Feichtner's radio stations followed their progress, and passed on their signals and estimated time-to-target by the minute. By the time they were over Ploiesti, every German fighter plane and flak unit in a 100-mile radius around the oil fields knew they were coming. The results were a bloodbath for the Americans: they lost fifty-three aircraft and 600 crewmen. Production at the oil plants was resumed within three weeks, and after a month had exceeded the output before the raid. Ferdinand Feichtner's careful preparations, technical knowledge and understanding of the implications for signals intelligence of the tactical and strategic situation had paid enormous dividends for both.

The failure of the raid, however, did little to ease the increasing pressure on the Germans across the whole of the Mediterranean; the Luftwaffe's regional command moved from Athens to the port of Thessaloniki, further north. The intercept out stations in Crete, the Dodecanese and the rest of the Aegean stayed where they were as the Germans moved to reoccupy these islands. As Feichtner himself took three of his companies to Thessaloniki, fighting began around his 'summer house' on the Loutsa promontory. The Greek National Liberation Front sided with the Germans, and went head to head with the fighters of the Greek People's Liberation Army. The country was falling apart. Feichtner called Italy's capitulation a 'betrayal', and saw the Third Reich collapsing slowly but steadily from the south upwards. American and British bombers were now moving their bases steadily further northwards as the Allies advanced up Italy, and so targets in Germany were now within flying

range from the south.

Signals Interception in Italy

While Feichtner concentrated on the air above him, filled as it was with crisscrossing Allied aircraft, other signals intelligence units from both the German air force and the army were also concentrating on the Mediterranean. A twenty-four-year-old corporal called Hermann Reudelsdorff operated in one of these units. A former economics student who had studied at the Sorbonne, he had been working in signals intercepts since 1940, when he was posted to Athens. Trained as a cipher clerk, cryptographer and interpreter, he was independent and self-serving, and not cut out to be a junior NCO in a strictly hierarchical German Wehrmacht unit. But that is what he had become, and for a time his prospects looked bright; in summer 1942 he managed to become a reserve officer candidate. He was posted to Belgrade with an army signals intercept platoon to try to start reading into the traffic of Marshal Tito and his Yugoslav partisans. The unit operated together with a long-range and short-range intercept platoon, and had one officer and twenty men, five of whom worked in cryptanalysis; they had a reputation among other army units as being the best when it came to cracking radio traffic encrypted and transmitted in Serbo-Croat.

The platoon was transferred under the command of a Wehrmacht KONA in October 1943, and then, for Corporal Reudelsdorff, things seem to have started to fall apart. His file says he was demoted to private and given a nine-month suspended military prison sentence. By December 1943, as the Allies were fighting their way through the Gothic Line defences in northern Italy, he was detached to one of the intercept units of Second Panzer Army in Yugoslavia; by January 1944, he was sentenced to death for complicity in a friend's desertion. This sentence was later quashed for lack of evidence, so he was sent back to Italy, to an intercept unit of the 29th Panzergrenadier Division, codenamed 'Renate'. Although he might not have been suited to the rigid structures of military life, the corporal was evidently a good interpreter and a clever signals analyst.

In Italy, when his unit moved into the line opposite Allied units, the first thing they tried to do was ascertain which formations they were up against. The British radio nets would often send messages in clear, giving the map coordinates of the units in front of the German ones. They had the habit of

using phrases like 'big boys' for tanks and 'big sunray' for divisional commander. From the messages they sent, on frequencies which did not change, the Germans could work out which units were deployed opposite them in the line. Prior to an attack, the British often sent messages such as '*Are your big boys ready to start?*' By Christmas 1944, the 29th Panzergrenadier Division were holding a position on the River Senio at Bibbiano, forty miles north-west of Bologna. Their intercept platoon overheard two British officers discussing an impending attack two hours before it started, in clear, without any form of encoding: the Germans opened up with artillery fire, the attack was repulsed, their senior officers were delighted by the intercept platoon, and the signals monitor in question was decorated.

The Strategic Side Effect of the Fighting in Italy

The British wanted to use the Dodecanese islands as spring-boards for possible amphibious operations in the Adriatic, and even an invasion of Yugoslavia. The problem was that Eisenhower's strategic diktat forbidding the diversion of forces meant that British operational capacity was limited to a few battalions of paratroopers and infantry, and the buccaneering special forces of the Special Boat Squadron (SBS) who saw the Aegean as an operational fiefdom in which they could cause as much havoc as possible.

A German brigade took Rhodes, but the British then made landings on several of the other Dodecanese islands, hoping that in conjunction with the Italian forces already based on them, they could stage a counter-attack on Rhodes. The operation on the island of Kos, four miles from the Turkish coast, proved them wrong. On 13 September 1943, American bombers attacked the three Luftwaffe bases on Rhodes in an attempt to ground the German fighters and bombers based there. The attack was temporarily successful, and the lull in German air dominance saw British and Greek special forces land on Kos and take the port and the airfield near the village of Antimachia. This enabled Spitfires flown by South African pilots to land on the island, and then on the following night a company of British paratroopers jumped onto a hastily arranged drop zone, and formed an immediate defensive perimeter. Delighted to see them, the Italian soldiers on the island reportedly laid straw on the airfield runway to soften their landing. The problem was that because of the Luftwaffe's comprehensive network of signals intercept outposts, radar stations and decryption experts in both Germany

and Greece, every move the British made could almost have been broadcast in clear on every radio frequency in the Mediterranean.

The Germans counter-attacked two days later, reduced the airfield runway to pitted chaos, and interdicted the attempts by the British to land a battalion of infantry from Syria. Most of these men from the Durham Light Infantry made it onto Kos, and fought to establish defensive positions under heavy German bombing; then the Germans transferred another seven squadrons of aircraft to the Aegean, bringing their total up to 360. The Allies were hopelessly outgunned and outnumbered.

Dawn comes early in the Adriatic in the autumn, and as the sun arched into the sky on 3 October, German paratroopers from the SS and Brandenburg Division special forces dived out of Junkers transport aircraft at low level. The limestone rocks, the sandy gullies full of olive trees and the salt flats outside the town of Kos made for a hard landing. The way a German parachute harness was configured meant that when he landed one of the first main points of impact for a *Fallschirmjäger* was his knees, and then his furled arms, shoulders and back. Given that the temperature inside the packed transport aircraft was stifling, and the men were carrying heavy equipment, it meant that when they landed they and their uniforms were drenched in sweat. Rolling immediately on hitting the drop zone, they went into battle covered in dust, sand and salt from the flats, as though rolled in flour.

By dusk the outcome of the battle was a formality: although the British infantry and special forces fought desperately, German air cover, light artillery and superior numbers won the day. By 6am on 4 October it was over, and 1,400 British troops and some 3,100 Italians were taken prisoner. The British went to German POW camps, while a few evaded capture and, with the help of canny SBS troops, were evacuated from the island. The Germans decided to make an example of the Italian commander and his officers, payback for their betrayal during the Armistice. There were 148 officers, and seven decided to switch allegiance to the Germans. Thirty-eight, seeing what was coming, escaped. The remaining 103, including their colonel, were told to pack suitcases and make their way on foot to a ship in the port, walking in a long line across the dried grass and through the rugged olive trees near the village of Linopoti. Then they discovered that there was no ship waiting on the dark cobalt sea, and that behind them their German captors had formed a line and were feeding belts of ammunition into their MG-42 machine guns, and cocking their Schmeissers. The bullet-riddled corpses of the Italian

officers, sticky with hot blood, were buried in shallow graves in the hard, rocky ground.

Losing Kos meant the British also lost the other key islands in the Dodecanese; the Germans took Leros a month later, their complete air supremacy a major contributing factor. This supremacy was achieved in large part because Luftwaffe pilots, flight controllers and air crews knew what enemy aircraft faced them, when, where and coming from which direction at which time. They were well briefed and well prepared, and this was entirely the result of their signals intelligence network in the eastern Mediterranean, both cryptanalytical and that based on radio direction-finding and radar. The architect of this, Major Ferdinand Feichtner, was meanwhile about to depart for another theatre of war where the Luftwaffe enjoyed no such superiority. Normandy.*

In his post-action analysis of the fighting in the Dodecanese, British Admiral Andrew Cunningham said simply that the Allies failed because they were unable to establish airfields in the area of operations: 'The enemy's command of the air enabled him so to limit the operations and impair the efficiency of land, sea and air forces that by picking his time he could deploy his comparatively small forces with decisive results.'[2]

---

* Major Feichtner's activities in Normandy are described in Chapter 21.

Chapter Twenty

INSECURE ENIGMA

Nearly ten years before the outbreak of World War II, the Germany navy realized that ensuring the security of its communications infrastructure was going to be vital when the country went to war. Securing this meant securing the physical means used to transmit information, and for the Kriegsmarine, this meant keeping their Enigma machines and their settings confidential and physically safe. In January 1930, the OKM, the Kriegsmarine High Command, sent a list of security measures to each of its major sub-divisions such as the surface fleet, the U-boats and others. It conducted a survey amongst its four major units that stated: 'A surveillance of the machine and the rotor box, more comprehensive than before [particularly on smaller vessels], is planned … a sharp supervision of personnel who have access to the machine is necessary …'[1]

The Enigma was from then onwards to be kept at all times in a box or compartment or drawer that was locked, not just held closed with a lead seal. One battleship captain said that his Enigma machine was kept in a specially prepared, lockable cabinet of the cipher desk in the radio room, while the rotor boxes were kept in the cabin of the radio officer in a separately locked compartment. On 15 October 1934, the Wehrmacht High Command distributed a memo on Personnel Security, which reminded all units and everybody in them of the importance of taking care of secure communications equipment:

> During a change of position … a non-commissioned officer and a private of a communications battalion left, through negligence, the cipher machine and the hand cipher in the field. The loss was noticed by them upon arrival in their new position, but the material was not found in the place where it was lost. A civilian had taken it and delivered it to the mayor of a neighbouring village within half an hour.[2]

In the same memo was a list of servicemen and women who had been executed for treason and betrayal of military secrets. There were 148 of them in 1933, and 155 in the first seven months of 1934. In this period, a number of people were also discovered to have been 'negligent', and the list included a certain Radioman Second Class Egon Bress of the 4th Torpedo Boat Half-Flotilla, who was arrested in February 1934 for taking photographs of Enigma and hundreds of cryptographic documents for his own uses.

On the one hand it was obviously vital that the actual Enigma machines and their component parts, such as rotors, were not lost or stolen or handed to enemy agents, but another form of security consisted of assuring that the machines were used in the right way. On 9 January 1932, Radioman Kunert, who was based in Kiel on the Baltic, made the basic error of sending the same message both encoded and in plain text, thus giving away the current settings of the Enigma machine he was using. The navy then started to print its confidential documents in a water-soluble ink, as well as a normal one, before realizing that exposure to damp air on ships would cause any form of ink that was not oil-based to run.

Yet the most important security measure put in place before the outbreak of war was designed to keep Enigma secure should the machine, its rotors, its codebooks or its daily or weekly or monthly keys be stolen or captured. If this happened, the cipher clerk who discovered the loss was under strict orders to change the rotor settings – if the machine had not been removed – and was to change the order in which the rotors were placed in the machine. The order in which he inserted them would obviously be confidential, and he would have to let any recipients of his messages know that emergency resetting of the rotor order had taken place, meaning that the security of the previous settings could now be considered compromised. To do this, a special indicator word would be used at the start of each new message, telling the recipient that pre-chosen security changes had been made, with the details to be found in his codebook. One of the first words used to indicate this was

'Aldebaran'. The use of this word meant that whoever received the message went to a section of his codebook, where a series of instructions would tell him how to reconfigure his machine.

The Wicher Plan

In 1939, when they reached Warsaw, the Germans searched the headquarters of the Polish cipher bureau, the Biuro Szyfrów, which was part of the Polish General Staff's Second Department. They captured a number of encrypted and plain text documents, including those from a German cruiser operational off Spain. They found the plain text version of a wireless transmission that had been transmitted from a German naval ship operating during the Civil War. This had been sent using the Enigma '*Offizier*' key, which suggested either that the captain of the cruiser was working for the Poles –highly unlikely – or, far more probable, that the Poles were able from 1936 onwards to break some or all of the German codes used on their naval Enigma, which seemed to suggest that the Enigma system was compromised.

Shortly afterwards, a group of Polish staff from the bureau who had fled to Romania and then Czechslovakia were captured by the Czechs. Their military intelligence organization contacted OKW-Chi, and Walter Fricke and one other man then travelled to Czechslovakia and interrogated them: the Poles said they had broken Enigma before the war. The documents the Poles had with them were sent back to Germany to one Captain Kempe of OKH; Kempe did not get on, at all, with Wilhelm Fenner, who was thus not shown the documents, but only told that from the evidence contained within them it was clear that Enigma had been broken. Lacking hard evidence for this, as he hadn't seen the documents himself, his reaction was that security of the Enigma encoding infrastructure should subsequently be increased. From the beginning of 1940 it was.

The operation that was to lead into an extended investigation into the possible compromise of Enigma by the Poles before the war became known as *Fall Wicher*, or Case Wicher. The name was derived from the Poles' name, found in captured documents, for the plan carried out by their cipher bureau that was supposed to have broken into Enigma. In Polish it was *Wicula*, meaning 'gale', but the Germans changed it to Wicher.[3] A post-war American security analysis offered an explanation about German rationale for why they believed that Enigma had been comprised but that there was no operational

liability:

> The key to German suspicions of Enigma appears to have been the knowledge of Polish pre-war successes, after which the wartime Enigma exploitation hung by a thread for five-and-a-half years … the Poles who disclosed the success were too high up in the Warsaw Cryptography Bureau to know how it was done – those who knew were not captured or interrogated. German cryptographers were never forced to an understanding of how the machine could be solved. They were told, not shown.[4]

The Germans meanwhile captured two more Polish officers after the fall of France in 1940; they were sent to a POW camp and interviewed, but initially the Germans did not know that they had held senior positions in the Warsaw cipher bureau, and that they had been respectively a lieutenant colonel and a major. By the time further interviews were conducted in 1942 and 1943 in Warsaw and Berlin, a colonel from OKW-Chi said that one of them was a lieutenant colonel and head of the cipher bureau itself. By this stage the two officers were in a POW camp outside Hamburg, and had told the Germans simply that the Poles had been reading Enigma for several years before the war.

Further Investigations into the Security of Enigma

When the German commerce raider *Atlantis* was sunk in 1941, the Kriegsmarine's headquarters carried out an inquiry, which declared that neither the Enigma system nor its users – in this case naval officers on the *Atlantis* – were at fault and Enigma was still to be considered secure. Wilhelm Tranow, however, was concerned that the German reliance on one machine system that was used by the army, navy and air force could lead to substantial problems with communications security. He had seen in World War I how vulnerable the use of codebooks made the German navy, and his decryptions of the British Royal Navy's codes from their own cipher texts simply confirmed this. He wanted the Kriegsmarine to adopt a three-part system based upon Enigma, physical hard-copy codebooks and enciphering tables which changed frequently, and possibly a telex-style machine. A German called Fritz Menzer invented a cipher device that he called SG-39, which had

270,000,000 permutations of setting, but it was costly, it was delayed, and by 1939 only three were ever made.

By this time the entire German armed forces at sea, in the air and on land were using Enigma: replacing the entire communications system of an infrastructure consisting of several million people was too huge an undertaking, especially on the eve of war, and especially when there were no proven examples of Enigma being compromised. The Germans assumed throughout the war that introducing more rotor settings on the machine and changing the key settings of each different code would make them impregnable. A fundamental assumption they made was logically simple: if they were reading parts or all of different British codes at different times, and no mention in any signal was ever found that referred to any material transmitted by the Germans in an Enigma-enciphered message, then the system had to be secure. In 1942 one of Admiral Dönitz's staff officers read an intercepted Royal Naval signal from the British Admiralty's Submarine Tracking Room, located underground near the top of the Mall in London. It referred to the B-Dienst's capability to read some British naval codes, and warned that it *had to be assumed* that the German submarines and their colleagues in naval intelligence could read some, if not all, of the Royal Navy's and Merchant Navy's encrypted signals. It was this information that was passed on to the captain of the *Ottowa* by Commander Peter Gretton, at the enquiry that took place after the sinking of the Canadian destroyer by U-91. While this did not tell the Germans that the Allies were reading messages enciphered with Enigma, it warned that the Allies *knew* that the Germans were reading some British naval signals; and because they knew this, the German logical deduction could have been that the British could be deliberately avoiding making any reference of German Enigma in any of their coded communications. Simultaneously, Major General Wolfgang Martini, the head of the Luftwaffe signals intelligence service, said that Enigma could only be considered 80 per cent secure.

For the Germans, Enigma's security was about assumptions of secrecy and technology, as well: if the British were so visibly dependent on codebooks for the whole war, then German reasoning said that it was because they were technically incapable of inventing a mechanical system that could equal Enigma. The British Typex machine* found on the beach at Dunkirk was all the proof they needed: they thought it a primitive cousin of Enigma, and it was clear to them that the British were not using it to transmit signals,

because if they were, then wouldn't the German chain of listening stations have intercepted some of the messages encoded with it? It was only in October 1942 that OKW-Chi decided that, due to the high possibility of Enigma machines being lost during the fighting in Russia, very clear action should be taken not just to ensure the security of the system, but to allocate a particular person or persons to do this. The Kriegsmarine's security overview came directly from Admiral Karl Dönitz, but Wilhelm Fenner's organization chose a twenty-four-year-old mathematical logician called Gisbert Hasenjäger.[5]

His father was a lawyer and local politician from Mulheim, in the Ruhr, and Hasenjäger only finished school in 1936, before being conscripted into the army, serving in an artillery unit in Russia. He was badly wounded in January 1942, and spent nine months recovering after which Heinrich Scholz, a German logician, suggested he went to work with Wilhelm Fenner. He joined the section which oversaw the security of OKW-Chi's own ciphering systems, including that of Enigma. Having attended a cryptography training course given by Erich Hüttenhain, he was put into a newly formed department, whose principal responsibility was the defensive testing and security control of their own methods and devices. Hasenjäger was ordered to examine the Enigma machine for cryptologic weaknesses, and the particular model that he examined was a variation that worked with three rotors and had no plugboard.

The machine Hasenjäger was presented with was technically a much earlier version of Enigma than that which was being used, by then, on the Russian Front or on U-boats. He was given a 100-character encrypted message for analysis, and found a weakness which enabled the identification of the correct wiring rotors and also the appropriate rotor positions, so as to decrypt the messages. Further success eluded him, however. He crucially failed to identify the most important weakness of the Enigma machine, which was the lack of fixed points, of letters encrypting to themselves due to the reflector. This was, after all, one of the most basic underlying principles of the Enigma machine, namely that no letter could be encrypted as itself. Because he missed this, it made his further investigations into the system redundant, but OKW-Chi and by extension the entire Wehrmacht High Command (though not the Abwehr) took his subsequent report as solid proof that Enigma had not been compromised.

As a result of the security investigation into German ciphers and the

reporting of new discoveries, the *Referate* of the Wehrmacht began to develop new cipher security techniques of their own, and in 1942 the development of these techniques was handed over to OKW-Chi, although after the July Plot of 1944, the RSHA, on Hitler's reported instructions, specifically banned it from intercepting and attacking any German traffic as a security precaution. So the main investigation carried out by the Mathematical Referat of OKW-Chi and then the GdNA was a continual enquiry into the security of the different ciphers used by the Enigma machines.

When it came to the Poles, this instance of compromise affected the plugboard Enigma and obviously not the commercial model; but it was only in 1943, and 1944, that General Erich Fellgiebel ordered the re-interrogation of the captured Polish cryptanalysts to check this point. Nevertheless, these investigations revealed that the safety margin of the Enigma cipher machine had to be reduced from 50,000 to 20,000 letters on a day's cipher: this meant that some messages or message chains had to be split up into three or more portions. In March 1944, the OKH stated that the existing naval Enigma security procedures were totally inadequate from a point of view of security: 'Retaining the present key techniques, five message keys chosen by specific agreement are sufficient to betray the daily key without permitting the German control agency to spot the betrayal even with careful checking.'[6]

Wilhelm Tranow and the B-Dienst were much more conscious of Enigma's vulnerability than the Wehrmacht, but each time there was a fear about its security, as in February 1942, they either added another rotor or changed the machine's key codes. By November 1943, American and British bombing raids had forced Tranow and his team to move out of Berlin to a new location near the town of Eberswalde, about twenty miles north of the capital. The Allied bombing had also destroyed very large parts of the organization's physical paper records going back to the 1920s. After the German triumphs against their naval ciphers, and their long overdue security reviews in spring and summer 1943, the British Admiralty were now changing their code keys every day, instead of every fortnight as they had done the previous year. Along with the move of their headquarters, an increasing lack of personnel, the loss of their documents, and constant external worries about the Reich's internal security, this meant that suddenly the B-Dienst's access into the British navy's communications effectively came to a halt.

At the end of April 1944, two German torpedo boats sank the Canadian

destroyer HMCS *Athabaskan* off the far north-west of France; the explosion as the ship blew up could be seen twenty miles away. Not only did the German MTBs rescue as many Canadian sailors as they could carry, they also captured some of the latest Royal Navy codebooks, with an explanation of their new double subtractor system. To compound this success, when the Canadian prisoners had been taken to dry land in Brittany, one of their leading telegraphists gave his German captors a detailed description of the new double conversion procedure for the 'stencil subtractor' system. It was too little, too late. In May 1944, Hitler sent a confidential order to the B-Dienst. What English naval ciphers was it currently reading? The reply was almost none: the two main high-security English ciphers could no longer be read. For Wilhelm Tranow and his men, the successes of 1942 and 1943 suddenly seemed a long way away.

At the same time, the naval cryptographers ordered another review of Enigma security, and one analyst broke into the encoding system on a four-rotor Enigma on the basis of a crib of twenty-five letters. The test was carried out on a machine supplied by OKW-Chi, and both they and the navy's men decided the system was still secure. The reason for this decision was that both agencies were unable to conduct sufficiently deep security tests to determine how secure they were. They were also unable to put forth the costly practical effort required to solve them.

> Their security tests were theoretical only, and they were unable to imagine what a large concerted effort at traffic analysis could achieve. A security measure which would have proved productive was the issue of new Enigma rotors. However, so many Enigma machines were out in the field, that it would prove impractical to update them. OKW-Chi also felt that even if a particular Enigma unit was captured, it would still be considered secure, since no process was known by OKW-Chi that could break it.[7]

The message was clear: because we could not imagine a way by which the Enigma system could be compromised, then it was clear that nobody else could either. The Germans were displaying an increasing level of lack of technical imagination, as they could not see that mass-spectrum analysis of coded signals, like the Polish or British bombe system, could be invented. The Third Reich might have been listening, but increasingly it had its fingers

in its ears. Ferdinand Feichtner and Ferdinand Voegele had seen further, though, and insisted by mid-1944 that the Luftwaffe adopt the pluggable reflector to their Enigma machines, making the British use of bombes redundant. But Erich Hüttenhain, suggesting to his superiors that the German army should follow suit immediately, discovered an apathetic response. It is too much trouble, they said.

Out in the Atlantic, these decisions and developments were having very decisive effects. As early as April 1943, Allied convoys had suddenly begun to out-manoeuvre the U-boats, and the changing of the British naval codes reinforced this. On 16 April 1943 Convoy SC-127, with fifty-seven ships, sailed from Nova Scotia. The freighters were carrying tanks, grain, explosives, steel, timber, sugar, phosphates, and fuel oil. Its original route would have taken it through an area in which the British codebreakers at Bletchley Park had discovered an estimated twenty-five U-boats. Its course was altered so it sailed around this area of sea, shaped like a square, and eventually the convoy arrived in its British ports without the loss of a single vessel.

This Allied intelligence advantage was augmented by the growth in Allied air cover over the Atlantic. Some of this came from very long-range patrol planes, and these aircraft closed the black hole, the 'air gap' in the mid-Atlantic in which the U-boats had operated free from the fear of air attack. Flying over the convoy routes, the aircraft kept the U-boats submerged, greatly restricting their mobility and their effectiveness. More air cover came from planes flying off escort aircraft carriers. And these did something decisive and offensive, which turned the advantage in the Battle of the Atlantic firmly towards the side of the Allies.

U-boats in the Atlantic were supplied by Type XIV submarines, which were nicknamed '*Milchkühe*', or 'milk cows'. They were huge boats weighing nearly 1,700 tons, and almost 200 feet long. They liaised with groups of U-boats one at a time, and replenished their reserves of fuel, food and torpedoes; they had on-board bakeries so the German submariners could even have fresh bread in the middle of a combat patrol. In 1942, the supplies from these boats had extended the radius of the U-boat fleet to the extent that they were able to raid the eastern seaboard of the United States, in the period referred to by German captains as 'the American shooting season'. The 'milk cows' were obviously high-priority targets for the Allies, as sinking one would mean that at least six other operational U-boats would then have to return to France or Germany to re-supply, cutting short their combat patrols, meaning they

could attack fewer convoys. Of fourteen Type XIV submarines commissioned between 1941 and 1943, all fourteen were sunk or scuttled. Aircraft from escort carriers carried out an intensive series of operations against them in 1943 and 1944. In tandem with the B-Dienst's increasing failures to read into British naval codes, the closing of the 'air gap' and the fact that Bletchley Park was reading back into 'Shark', meant that in the run-up to the invasion of Europe more and more convoys crossed the Atlantic without being torpedoed. Between mid-December 1943 and mid-January 1944, U-boats sighted not one of the ten convoys that sailed close to their patrol lines, and sank only one isolated merchant ship. In the first three months of 1944, U-boats sank only three merchantmen in convoy, out of 3,360 that sailed. And the cost to the U-boats in this same period? Thirty-six submarines had been sunk. To compound this switch of the strategic and tactical advantage to the Allies, Wilhelm Tranow found that the Russian Front and civil emergency duties at home in Germany were depleting his staff again: by January 1944, the number of men and women he had available to decrypt British naval codes had dropped from its all-time high of 198, to just ninety-four.

---

* The Typex was a British rotor-based encryption machine, an adaptation of the commercial Enigma, developed by Wing Commander O. G. W. Lywood in 1934. After trials in 1937, the machine was adopted by the British Army, RAF and some government departments..

Chapter Twenty-One

THE COMING STORM

Operation Overlord

In September 1943, Major Ferdinand Feichtner went to Normandy. General Wolfgang Martini ordered him to make an evaluation trip to see exactly how the Luftwaffe signals intelligence units were preparing for the Allied invasion of Europe, which the Germans knew had to hit somewhere on the northern coast of France. Where, exactly, they were not sure, but their signals intelligence analysts and codebreakers were doing their utmost to find out. Air Signals Regiment 351 of the Luftwaffe were responsible for monitoring and intercept duties for the German air force across much of northern France; when the predicted invasion came, either across the Channel into Normandy or across the Pas de Calais, their duties would be to provide advance warning of the operations of the American and British air forces.

Feichtner flew from Athens: it was late summer in the Mediterranean, and the German Aegean and Adriatic island campaign against the British, Greeks and Yugoslavs was in full swing. He and his men were operating in field conditions, while installing new transmitters and providing monitoring of the Royal Air Force's operations over the Aegean, Adriatic and western Mediterranean. The Allies had taken Sicily in July, and had landed at Salerno two weeks before his departure for France. The Italian armistice had taken the Germans by surprise, but they had reacted swiftly, sending reinforcements

down from France, Austria and the Balkans into Italy. In the Mediterranean it felt as though three separate battles were being fought at once, as the Germans tried to re-take the Aegean islands, fought a savage guerrilla war against Yugoslav partisans, and simultaneously did battle against two American and British armies in Italy. Tired but alert, Feichtner could see that the Reich's war was in the balance: Germany was fighting in Italy and Russia, and very soon would come a third front line, the long-expected Second Front in Europe. So as he flew from Athens to Berlin, and thence to Paris, his thoughts were focused on how his signals intelligence units would cope.

He was not prepared for what he found. One of the units was based in a château outside Paris, which the men called the 'Signal Castle', or *Meldeschloss.* The surrounding gardens were kept raked and pruned and mown by a small army of French gardeners. Inside the castle was new electrical equipment, the rooms were spread with rugs, and comfortable, elegant curtains were drawn across the bay windows at night. Feichtner, in contrast, had for months been used to waking to the Mediterranean dawn, the shimmering slow-rise heat of Greece, and the buzzing cacophony of cicadas, before launching into active operational work that seemed to pour over the edges of each day it filled. Here in France, life was noticeably slower and more languid. Urgency did not seem to be a valid currency.

The commander of the 3rd Battalion of the regiment lived in the eighteenth-century splendour of the Château de la Celle, three miles from Versailles, south-west of Paris. In his operations room there was a huge map which had different coloured lights on it, each of which indicated the headquarters of different British and German signals organizations, the various broadcasting frequencies they used, the locations of radar intercept stations, and the bases of German infantry units and Luftwaffe fighter and bomber stations. By turning on the right switch, a coloured bulb installed inside the map would light up, indicating the base in question. The unit's commanders were also spending a lot of time putting together a picture book of signals intelligence, whose graphics Feichtner thought were like those of a child. This was the backbone of the preparations that one Luftwaffe signals intelligence regiment was making against the imminent Allied invasion of Europe. One of Feichtner's senior officers ordered him to make a similar picture book too, but he refused. He was far too busy, he said.

The hard-bitten German major noticed that a huge amount of work was being put into the lawns of the park which surrounded the castle. Feichtner

stayed at the castle for several days, and each morning observed that the green turf of the garden was criss-crossed by lines of brown mole hills. And each morning and evening, when their duty shifts finished, the non-commissioned officers and the private soldiers were ordered by the officers to go and fetch spades, after which they dutifully shovelled up the little earthen mounds until all that remained was the brown circular scars on the lawn, which showed where the industrious moles had surfaced. The NCOs and men would then flatten down the turf, take away the earth they had collected, and, the following day, do it all over again.

In the meantime, Feichtner realized that urgent operational matters were a mess. Only two out of twenty-five companies in the regiment, or 220 out of 2,700 men, had any form of mechanized transport at all. No training had started on any of the radio receiving sets for any of the operators, and none was due to start until the first week of June 1944. The battalion was based in forty-six separate villas in the neighbourhood, which made it effectively impossible to get hold of an officer or technician when the day was over. Feichtner had taken to sending one of his officers from either Berlin or Athens to visit this unit, under pretence of separate liaison visits. When he went to Normandy himself, he remarked that 'the unit had waxed fat in more ways than one … it had a supply of electrical fandangos to dazzle the eyes of the generals'. The different coloured switches on the map, he said, made him feel as if he was seeing a movie. Along with his own personal observations, his impression was one of what he called 'a horrible example of military decay'. Four years of life as occupiers of France had taken their toll. Feichtner suspected that tactical chaos and organizational collapse lay ahead for the unit, when the Allies arrived. If they were lucky.

German Signals Intelligence and Codebreaking in Normandy Before Operation *Overlord*

Not all of the Luftwaffe's signals intelligence work for the preceding four years had been confined to tidying lawns. Up on the Channel coast at Deauville, Lieutenant Martin Ludwig and his men knew by spring 1944 that the invasion was coming. They had been tracking the movements of the RAF and the USAAF on a daily basis since mid-1942: the build-up of squadrons in southern England was, by March 1944, greater than anything they had seen before. Up until that month, they had been able to follow the USAAF radio

transmissions, to identify the ever-changing RAF radio call-signs, and to be able to predict with some certainty where each bomber mission was heading to in Germany. The Americans would take off earlier than the British, as they conducted daylight bombing missions, and the latter mainly bombed at night. When the American Flying Fortresses were en route to, and over their targets, they would send radio messages back to their bases about flying conditions. How intense was the flak, was there cloud cover over the target, at what point in the flight did German fighters appear, and from where? These messages were then forwarded to British Bomber Command, to help them on their missions later on during the same twenty-four-hour period. From these messages, the Luftwaffe were often able to work out what was the British target for that night. They were helped by the fact that radio discipline among American bomber crews was, at best, occasionally observed, at worst non-existent.

By March 1944, exercises and practice missions in Great Britain had ceased. The last practice training operation that Ludwig's men monitored was codenamed 'Spartan'. Ludwig told his superiors several times that this meant that the build-up for the invasion had now gone beyond the final training stage, and moved into the phase immediately before a big operation where radio silence was imposed.

To get a clearer picture of which Allied units were doing what, where, how and when in southern England, the Luftwaffe could make reconnaissance flights over the Channel and the ports and towns of the south coast. The problem was that these were extremely risky: long gone were the almost halcyon days of Rhubarb and Rodeo. In spring 1944, if a Junkers Ju 52 with a reconnaissance team and a radio monitoring unit on board were to appear within range of any British airfield or port, four Spitfires would materialize, and tear it to pieces in minutes. Likewise any faster Focke-Wulf fighter or two-engined Dornier. The Germans tried a number of ways to photograph training areas, troop assembly points, harbours and airbases, using fast Messerschmitt Bf 109s, and even on one occasion a captured American P-47 Thunderbolt. But safe and effective ways of gathering up-to-date tactical and strategic intelligence were extremely limited. What Ludwig did know was that the number of Allied bombing raids on German radar stations and signals monitoring units was increasing, and it didn't seem to matter whether these were in the Pas de Calais area, Normandy or Brittany. He assumed, like many of his colleagues, that the Allies would be mounting an enormous deception

operation designed to mislead the Germans as to the exact intended location of the invasion.

German Reinforcements Arrive in Normandy

Ludwig knew that the OKW, the Wehrmacht High Command, thought it probable that either the Pas de Calais or Normandy would be the target. The Luftwaffe lieutenant and his men travelled through the roads of Normandy a lot that spring and early summer, their Kübelwagens and trucks rattling through the bocage hedgerows, as they moved from one radio monitoring site to another. They began to see signs of many of the new and different German units that had arrived in Normandy as reinforcements. Turning a corner on a road, they would suddenly see bivouacked troops, half-tracks, motorcycle combinations and tanks camouflaged with tree branches, vast stooks of early corn and long grass, or sometimes whole saplings. On the vehicles would be painted the divisional signs that announced who these new, determined-looking troops were. The crossed key and diagonal lightning flash told the Luftwaffe men that here were the 12th SS Panzer Division, the 'Hitler Jugend'. They were recruited predominantly from the Hitler Youth and then had their ranks strengthened with officers and NCOs brought in from other SS divisions, like the Leibstandarte Adolf Hitler. In March 1944, their commander was SS Brigadier General Fritz Witt.

The unit had not been slow to make its presence felt in France. One of the largest demonstrations ever made in the whole war by French workers had taken place in Lille in March, when 60,000 workers went on strike. Many German troops knew what lay behind the French outrage: it was the fault of the 12th SS, the 'Hitler Jugend'. The division had been en route to Normandy by train at the end of March 1944, near the junction of the French and Belgian borders, when they approached the station at Ascq, where three railways met. Suddenly, an explosion blew up the line directly in front of the SS soldiers, and two cars of the train derailed onto the side of the track. Immediately, the commander of the rail convoy, First Lieutenant Walter Hauck, ordered his men to search the houses on both sides of the railway and arrest any men they found. The SS then shot seventy of them; another sixteen were executed in the village of Ascq itself. After a subsequent Gestapo investigation, a further six men were shot by a firing squad. The unit's behaviour was a foretaste of things to come in the fields of Normandy.

Among the other divisional emblems visible in the Normandy countryside that spring were the elaborate italic 'L' of the Panzer Lehr Division, and the crossed 'D' of the 21st Panzer Division, which previously had made up half of the armoured component of the Africa Corps. Then there was the 352nd Infantry Division, spread along the coastline above Bayeux, and, further north near the Pas de Calais, the 2nd Panzer Division. For the Luftwaffe officers of the signals intelligence regiments, it suddenly became common to see other members of another branch of the Luftwaffe appear in their messes in the evenings, or out on manoeuvres in the countryside, or preparing fortified positions up near the Cotentin peninsula. These were Luftwaffe Fallschirmjäger, paratroopers who'd served in Crete, the Aegean, Italy and Russia, now deployed to Normandy. All together, there were 46,000 men in these newly arrived infantry and tank units alone, all reinforcing the Atlantic Wall.

Hitler's Opinions on the Coming Invasion

On 27 May 1944, the Japanese ambassador to Berlin, Colonel Hiroshi Oshima, had a meeting with Adolf Hitler. Oshima was a former army general who had proudly championed the cause of closer coordination with the Third Reich. He had first met Hitler in 1934, when he was the Japanese military attaché in Berlin, and he had built up a network of contacts with Germany's political, military and industrial leaders. He and Hitler had formed a close working friendship, and through the German foreign minister Von Ribbentrop the two men met regularly. After each meeting, Oshima would return to his embassy, and write a report. Like that other great source of information, Colonel Bonner Fellers, he was frank, thorough and indiscreet. And as with Fellers, the enemy were reading his messages. The Japanese diplomatic code – codenamed 'Purple' by the Americans – had been cracked two years earlier. American leaders often had the opportunity to read the intercepts before they even arrived in Japan, as telegram and radio communications between Berlin and Tokyo were often jammed, given the difficulties of aerial bombing raids, the war in Russia, and the increasing bombing of the Japanese capital. This meant communications could take much longer to reach Japan than America. One of the men who decoded the signals was to say in 1998 that the Americans often saw Oshima's signals before the Japanese did. Sam Snyder was born in 1912, and worked at the

signals intelligence agency on Constitution Avenue in Washington DC. He commented: 'We gave them good, clean copies with no more than a word or two missing sometimes. American leaders often had the opportunity to read the intercepts only two hours after they were sent.'[1]

And at the meeting on 27 May, Hitler told Oshima his concerns. Firstly, there was Italy, where he expected a large Allied offensive, in response to which the Germans would pull back to a series of defensive positions built across the Apennines. He thought the next Russian offensive would come in a two-pronged strike into Poland and Romania, and as for the invasion of Europe? The Führer thought there would be diversionary operations from the Second Front in Norway, Denmark and southern France, and after that the main attack would be made on Normandy and Brittany, with a subsequent strike across the Straits of Dover. Hitler added that, if the invasion did not come, he would blast England with 'rocket guns'.* In Russia, he said, the line was as static as it was when war started. The German leader said that Russian T-34 tanks were better than Germany's because of the terrain – the much-vaunted King Tiger had terrible problems in mud.

Oshima had made a four-day tour of the Third Reich's Atlantic Wall fortifications in November 1943, and made notes, which he duly repeated in his telegrams, of the numbers of men available in every German division, what weapons they had, and where they were based. He accurately described tank ditches as 'built in a triangular cross section with a span across the top of 5 meters and a depth of 3.5 meters'. He wrote about turrets 'built in a continuous line, close to the shore, each equipped with two or three machine guns as well as grenade launchers'.†

•••

The Chief of the Operations Staff of Oberkommando der Wehrmacht was General Alfred Jodl. His strategic and tactical assessments were backed up by the signals intelligence of OKW-Chi, the Luftwaffe and the B-Dienst. By April 1944 signals intelligence was providing him with too little information about where the invasion might be coming. He and his colleagues thought it would be on the Cherbourg peninsula or in the Pas de Calais. Unbeknown to him, the Allies were carrying out an enormous deception operation in England, even going so far as to mock up the physical presence of a fictitious American army based in the Home Counties that could be aimed to strike

across the Straits of Dover. Meanwhile the A-3 speech scrambler that was used on the Washington–London radiotelephone link yielded a few hints in conversations between Roosevelt and Churchill that an invasion was coming, but not where. General Walter Schellenberg of the SD security service – the intelligence service of the SS – saw a priority message in March 1944 between Winston Churchill and Roosevelt:

> Early in 1944 we hit a bull's eye by tapping a telephone conversation between Roosevelt and Churchill which was overheard and deciphered by the giant German listening post in Holland. Though the conversation was scrambled, we unscrambled it by means of a highly complicated apparatus. It lasted almost five minutes, and disclosed a crescendo of military activity in Britain, thereby corroborating the many reports of impending invasion. Had the two statesmen known that the enemy was listening to their conversation, Roosevelt would hardly have been likely to say good-bye to Churchill with the words, 'Well, we will do our best – now I will go fishing.'[2]

The Germans identified the codename for the Allied invasion in December 1943. The valet to the British ambassador in Turkey was a German spy, codenamed 'Cicero', paid by Berlin in forged British banknotes, and encouraged to steal and copy every document he could from his lackadaisical diplomatic master. Iliaz Bazna was born in 1904 in Pristina, in the *vilayet* or province of Kosovo, then part of the Ottoman Empire. He served in the French army when he was sixteen, and then spent three years in prison in France for stealing cars and weapons. He had an established track record of working for the diplomatic community as a bodyguard and driver in several cities in Turkey and France, before in 1943 he was employed to be the valet of the then British ambassador to Turkey, Hughe Knatchbull-Hugessen.

One day while his master was asleep or absent, or in the bath, Bazna took a key from his desk drawer. He pressed it into a tin of wax, and a copy was made. He then used it to open the box containing the ambassador's private papers. He photographed these documents, and sold them to the Germans through one of their diplomatic attachés. In December 1943 he had copied a document that carried the highest security restriction there was – it was only to be seen by those on the BIGOT list.[‡] This was the group of Allied commanders and politicians who were cleared to know the details about

Operation *Overlord*. The document that Bazna copied included a sentence that said that the British ambassador wanted to ask Turkey if it could use air bases in their country to maintain a threat to the Germans from the eastern Mediterranean 'until *Overlord* is launched'. [3]

The Germans Detect Allied Air Force Invasion Preparations

The Germans knew that the Allies had been gathering all the landing ships and landing craft that they could, from the Mediterranean to the south of France to Scotland and Northern Ireland. Lieutenant Ludwig and his men noticed that the call-sign of the US Ninth Air Force had changed, and was now similar to that of the British 2nd Tactical Air force, with whom the Americans would presumably be operating over Europe. Ludwig's men also saw that the codenames of the squadrons they were monitoring, and the call-signs of some of the fighters and bombers, were all converging on a number of air bases in southern England. These ran in a straight line from Tangmere and Ford in Kent and West Sussex, up in a 'dog leg' to Reading and Odiham west of London, and then diagonally west towards Exeter. The radio call-signs of the American Second Tactical Air Force had already been identified by mid-1943 by the Luftwaffe signals intelligence units. The call-signs of the 83rd and 84th Fighter Groups in Great Britain, and the 2nd Bomber Group, were consistently identified through the use of radio direction-finding against the radio stations of the particular airfields from which they were operating. So when the headquarters of the 2nd Bomber Group moved from near the Wash, in Lincolnshire, southwards to the area around Reading, the Germans had clear evidence that a concentration of air assets was now focused in southern England. The subsequent movement of both the 83rd and 84th Fighter Groups to the South Coast confirmed this.

The Flying Fortresses, B-24 Liberators, Lancasters, P-47 Thunderbolts, Mustangs and Spitfires whose call-signs Ludwig most frequently intercepted were now joined by another type of aircraft. In March, a new radio network appeared, broadcasting on a frequency that Ludwig's unit monitored; using radio direction-finding equipment this was pinpointed to the area around Cottesmore and Grantham in Lincolnshire. This radio station was then identified as being the control centre in three subsidiary radio nets, centred on Exeter, Cottesmore and Aldermaston. And then, in ground-to-air radio traffic all over southern Britain, there suddenly appeared electronic evidence

of a large number of aircraft that did not belong to any known bomber formations. At first, the Germans thought these were simply more bombers, but then it became apparent, through monitoring the signals detailing their refuelling requirements, that these new aircraft all had two engines. What were they? Firstly, they seemed to be carrying out a shuttle service between a number of South Coast airfields, and secondly, many of them would take off, fly for strict, pre-determined times from their home air strips, and then turn around and return. The Germans suspected they were dropping paratroopers: they interpreted their movements as the transport aircraft taking off, dropping the men on practice jumps over drop zones (DZs) in southern England, and then returning to base.

Through reading the RAF's Bomber Code, the aircraft designation of C-47 was repeatedly mentioned; in another message the name of the 50th Wing appeared. Since Luftwaffe signals intelligence knew that the 51st Wing, based in Italy, was an air transport unit, it followed that the 50th should be the same. The Germans then began radio monitoring of a short-wave band of 500 kilocycles coming from RAF Fulbeck, an aerodrome near Grantham. C-47s would practise towing gliders, and messages between them and the gliders, on the same frequency, were exchanged:

'*Have you the glider in tow?*'

'*Can you see the match-box?*'

'*There is a nine-ship C-47 with gliders in tow.*'

The C-47A Skytrain was an American-manufactured transport aircraft, more than 5,000 of which left plants in California and Oklahoma between 1943 and 1945. It was more commonly known by the name Dakota. Squadrons, wings and groups hundreds-strong, with gliders, were now being deployed from Essex to eastern Cornwall. Each American or British air base had a number of radio call-signs allocated to it, and when a squadron of aircraft moved to another aerodrome, it took the call-sign of its operational base. Thus a squadron of Spitfires whom the Luftwaffe would have been tracking on an individual basis through their respective squadron call-signs would suddenly begin to use another series of identification codes. Ludwig and his men were therefore able to follow squadrons and their wing groups across the southern half of Great Britain. Regarding the Skytrains alone, the Luftwaffe officer had made a conservative estimate that the Allies might have 1,000 of these, each capable of carrying twenty-eight fully equipped paratroopers.

The RAF 38th Group, meanwhile, sent messages enciphered in the

Bomber Code, from their base at Netheravon in Wiltshire, whose station call-sign was 9 Whisky Zulu. They too were carrying out practice air-landing operations with freight-carrying gliders, and paratroopers. The Luftwaffe's signals intelligence units then intercepted radio traffic in May 1944 that told them that the embarkation phase of the invasion had begun, after cryptanalysis carried out both by Ferdinand Voegele and by one of Major Feichtner's men at La Celle. This showed that signals communications were now established between the RAF's ground-air support parties, and the navy and air force personnel based on ships in the invasion force whose task it was to liaise with them. Radio direction-finding triangulated these support parties and ships near Plymouth and Southampton. The invasion, Ludwig knew, wherever and whenever it came, was going to be big. At the end of May 1944, the headquarters of the Luftwaffe's signals intelligence regiment at Asnières, outside Paris, issued a direct invasion warning:

> All preparations by the British and American air forces are complete. Two British and two American Close Support Corps for the support of four armies are available. The embarkation of Air Force Staffs has begun. The beginning of a large scale landing must now be reckoned with any day.[4]

On the basis of the German Luftwaffe's signals intelligence, and the target areas of Allied bombing, the estimate was that the invasion would come between Calais and Cherbourg. This was 290 miles. It was a lot of coastline.

The Invasion Begins

The invasion itself was picked up during the night of 5–6 June when, shortly before midnight, 100th RAF Group began an intensive operation aimed at jamming the German radar stations on the Channel coast; the jamming 'blanket' moved from east to west, so it was obviously hiding a large formation of ships. Weather reconnaissance for the 8th and 9th Bomber Groups in England began far earlier than was usual for an RAF bombing operation, and then the approach of the invasion fleet was carried out under strict radio silence. Just before midnight on 5 June, six RAF Handley Page Halifaxes cast off six Horsa gliders, carrying British airborne troops from 2nd Battalion Oxfordshire and Buckinghamshire Light Infantry. Below them in

the dark was France, and their target, the bridges over the Caen Canal and the River Orne. Between 12.15 and 12.20am the gliders hit Norman soil. Operation *Overlord* had begun.[5]

At midnight on 5 June, Martin Ludwig and his men were awake and on full alert in their headquarters at Deauville, fifteen miles east of the Allied invasion beaches. The entire signals intercept and radar apparatus of the Luftwaffe in the whole of northern France was going mad. German radio discipline was falling to pieces. Commanders were reporting in clear their men's sightings of Allied paratroopers, daily codes were forgotten by some, strictly adhered to by others. From north of Caen to the Cotentin peninsula, a blanket of radio confusion took over. And then, at dawn, Ludwig and his men listened as high-speed, urgent messages came in from German gun emplacements manned by men of the 352nd Infantry Division on the coast behind Vierville-sur-mer. Looking out from their positions over the sea, as dawn broke they could see ships stretching from one end of the horizon to another. Then any sense of morning calm or quiet was blown over the horizon when Allied battleships and cruisers opened fire, in a bombardment that blew high-explosive steel shells up to fifteen miles inland. Next there was a strange silence. Ludwig and his men had, by then, started packing their radio monitoring equipment into vehicles outside their headquarters, preparing to pull out and move west. Before they did so, they heard the signals coming in from the machine-gun positions of the 352nd. Landing craft, hundreds of them, were coming straight at them through the surf. Unknown to them, one of the sections of coast in front of the German infantrymen's concrete emplacements was a key Allied target, and it had been given a codename by American planners. It was Dog Green Sector, Omaha Beach.

As Ludwig and his men headed north-west in their trucks that day, towards Le Havre, with a view to being eventually withdrawn back to Germany, the lieutenant reflected that it was the second Allied amphibious operation he had witnessed in two years. Prior to both, he and his men had known clearly, from their radio signals interception, that something was coming from across the Channel. At Dieppe, they had known an operation was imminent, though they had not known about its precise intended target until the Canadian troops arrived off the beaches, and Ludwig and his men started intercepting their radio messages. The German artillery, mortar and machine-gun positions, their air superiority and complete command of the strategic

and tactical situation had then done the rest. They were in a perfect position where they had radio intelligence from signals and cryptanalysis, and the decisive means to operationally act on it.

In Normandy, they had the signals intelligence, but were woefully under-equipped to do anything with it. In the days and weeks after 6 June, this was the case time and again. On 7 June, German soldiers found a deserted, bullet-holed American landing craft that was drifting in the bullrushes of the estuary of the River Vire, west of Omaha Beach. Inside there were discarded haversacks and map cases. One of them contained a codebook, which detailed the daily key settings for the days of 6–12 June of the M-209 Hagelin enciphering machines used for tactical communications by the American 101st and 82nd Airborne Divisions. In tactical and strategic theory, this should have given the Germans the upper hand in fighting against these airborne soldiers in the first days of the invasion. It didn't, because they didn't have the armoured resources to take on the Sherman tanks of the American 1st and 4th Infantry Divisions. The tanks and men of the 12th SS, the 'Hitler Jugend', fought exceptionally – one British tank officer who went into battle against them said they were arrogant, ruthless, brave and tactically brilliant.[§] But this could not translate into operational success if they did not have enough fuel for their tanks, or if they were pinned down in the bocage hedgerows by British Typhoon fighter bombers, with no Luftwaffe air assets to fight them off. And what became of the Luftwaffe signals intelligence unit living in and around the Signals Castle at La Celle? When D-Day arrived, as Captain Feichtner later learned, the regiment went entirely to pieces, and either lost or had to destroy most of its equipment, before being captured or fleeing.

---

[*] Hitler was referring to V1 and V2 rockets.

[†] Other declassified documents, says the same newspaper report from 1998, show that Oshima attempted to mediate a separate peace between Russia and Germany after the huge Nazi defeat at Stalingrad in 1943 – and that Hitler seriously entertained the idea. With Germany stunned by the loss and a protracted conflict looming, Oshima approached the Germans with the idea, which would free Nazi troops to concentrate on the Western Front. According to Oshima's report to Tokyo, Hitler said he would make peace if the Russians ceded Ukraine to the Reich. He claimed he needed the rich resources of Ukraine to win the war in the

west. And Hitler's meeting with Oshima in May 1944 was where Hitler stated most clearly that he expected the Allies to launch their Second Front in Normandy and Brittany.

‡ A security clearance above 'Top Secret', it stood for 'British Invasion of German Occupied Territory'.

§ The author's father commanded a troop of four Cromwell tanks of the 15th/19th Kings Royal Hussars in Normandy.

Chapter Twenty-Two

EXECUTION AND CAPTURE

On 23 June 1944, the Red Army launched Operation *Bagration*. Named after Pyotr Bagration, a Russian general during the Napoleonic campaigns, the aim of the operation was to destroy the German Army Group Centre in Byelorussia, and push towards Poland and Romania. In five days of fighting, the Russians destroyed the German Fourth Army and most of the Third and Fourth Panzer Armies: 250,000 German troops were killed in a month. Minsk was liberated on 4 July, and the operation contributed to the end of German resistance not just across Byelorussia, but all of the central Ukraine. During July and August the Red Army continued to push the Germans back towards the Baltic, into Poland and Romania, and then the Russians reached the River Vistula and Warsaw, putting them in striking distance of Berlin.

On 20 July, Hitler and his inner circle of military staff and advisers went into the briefing hut at the Wolf's Lair headquarters, at Rastenburg in East Prussia, to hold one of a series of meetings to decide what to do about the disastrous strategic situation in the east. Normally, the meeting would have been convened in an underground, bombproof bunker, but it was too hot underground that day, so the outside hut was used. Colonel Claus von Stauffenberg, an aristocratic army officer who had lost his right hand, left eye and two fingers in action in North Africa, attended the meeting. Just before it began, he made an excuse, and left, leaving a briefcase containing a bomb under the table near Hitler. The following enormous explosion killed three

officers and a stenographer, and injured everyone else present.

The 20 July plot was a carefully planned *coup d'état* attempt against the Nazi regime, coordinated, planned and executed by an enormous group of army officers and civilians who wanted to assassinate Hitler, seize power in Berlin, establish a new pro-Western government and save Germany from total defeat. Hitler, however, survived, as just before the bomb exploded one of his officers moved the briefcase further under the table, behind a thick wooden table leg.

Not knowing that the Führer had survived, the coup plan went into action, and one of its priorities was to cut off all communications between the Wolf's Lair and Berlin. Responsibility for this rested with General Erich Fritz Fellgiebel, who was in charge of signals and communications at the Wehrmacht High Command. This put him directly in charge of their codebreakers, of Wilhelm Fenner and the teams at OKW-Chi. The attempt to cut off telecommunications failed, as Hitler's contingent of SS bodyguards had a separate communications network directly to Joseph Goebbels. The RSHA had for five years resisted attempts to put all of Germany's cryptanalysts and signals intelligence experts under one umbrella organization, specifically for this reason. They feared that if there was an attempt made on Hitler's life, Wehrmacht officers sympathetic to the plot would be able to take over Germany's radio, telephone and cryptanalytical links, effectively sidelining the SS and SD.

When he heard that Hitler was still alive, Fellgiebel telephoned another co-conspirator, General Fritz Thiele at the Bendlerblock, the signals headquarters in Berlin. '*Etwas schreckliches ist passiert*!' he reportedly said. '*Der Führer lebt!*' ('Something awful has happened! The Führer lives!')

Fellgiebel was then arrested immediately at Wolf's Lair and tortured for three weeks, but he did not reveal any of the names of his co-conspirators. Charged before the Volksgerichtshof, or People's Court, on 10 August, he was found guilty, sentenced to death, and on 4 September executed at Plotzensee Prison in Berlin. Seven thousand people in all were arrested, as the SS, Gestapo, SD and Hitler's security staff decided to root out any possible remaining opposition to the Führer. A total of 4,980 were executed, some of them slowly strangled with piano wire, on Hitler's specific orders, while others went to the guillotine.

Erich Fellgiebel, OKW-Chi, and Resistance to Hitler

Erich Fellgiebel was a major in the German army's signals corps in 1929 when he became the head of the Chiffrierstelle, the codemaking and codebreaking bureau of the Reichswehr, which would go on to become OKW-Chi. He was part of the team who decided to introduce the Enigma machine, and was adamant that Germany needed a single and coordinated cipher agency, but all his efforts were blocked by the foreign minister Joachim von Ribbentrop. He believed that the most effective way to forestall any possible resistance to the Nazi Party was by dividing its secret communications infrastructure as much as possible and encouraging and maintaining a climate of distrust among them. As has been seen, he, Himmler and Göring did this very effectively. Fellgiebel was made a general in 1938, appointed chief of the army's signal establishment and chief of the Wehrmacht's communications liaison to the High Command, or OKW, and on 1 August 1940 he became General of Communications Troops. When he was arrested he was Germany's most senior signals officer. He was party to every technical secret of the Third Reich, including the work on V1 and V2 rockets, and as Fellgiebel was seen to be part of a social and professional class in the military that included the Abwehr's chief, Wilhelm von Canaris, Hitler did not trust Canaris either. And he was right.

OKW-Chi and the Lucy Ring

By the beginning of 1944, there was a small and concentrated network of German officers and civilians in Germany who were attached to what had become known as the 'Lucy Ring', a conspiracy of Germans, Russians and others who passed information to the Soviet Union and were active in organizing resistance to Hitler. In Germany itself they included Major General Hans Oster, the chief of staff to Admiral Wilhelm Canaris, the head of the Abwehr; Erich Fellgiebel himself; his deputy at the OKW, Lieutenant General Fritz Thiele; Colonel Rudolf von Gersdorff, chief of intelligence at Army Group Centre; and Colonel Fritz Boetzel, the chief of intelligence evaluation at Army Group South-East in Athens, who, as we saw earlier had made several trips to Switzerland early in the war. Civilian members of the ring included Hans Bernd Gisevius, who was the German vice-consul in Zurich and an Abwehr officer. The members of the Lucy Ring in Switzerland itself were a rather less distinguished and rather less effective group of people, whose overall aims – passing information to Russia and resisting Hitler – were

considerably more grandiose than the actions they took to achieve them and the manner in which they carried them out.

The ring was named after the Swiss city of Lucerne, which sits in the German-speaking part of central Switzerland. It was run by a German refugee called Rudolf Roessler, who ran a publishing firm called Vita Nova that sometimes published anti-Fascist literature. Swiss military intelligence, led by Colonel Brigadier Roger Masson, used him as an asset, working with a press cuttings agency which was really an operation funded by military intelligence. General Fritz Thiele approached him in 1940, to pass on information about resistance to Hitler, and to do this gave him an Enigma machine and a radio, and a designation as a military signals station codenamed RAHS so they could send him covert messages without attracting suspicion. As these were sent from the German military's signals headquarters in Berlin, run by Thiele and his colleague Fellgiebel, they were never noticed. The information that the Germans passed to Roessler then went on to Swiss military intelligence, and to its head Roger Masson. He in turn passed some of it to the British, while a colleague of Roessler's called Alexander Rado passed it to the Soviet GRU,* the Russian military intelligence organization for whom Rado was operating. As he received the information from Roessler via a cut-out third party, he codenamed this person 'Lucy' after the city of Lucerne.

Did the Lucy Ring let the Russians know in advance about Operation *Barbarossa*? Were they instrumental in passing on information from the German signals generals in Berlin about the impeding attacks on Case Blue, Hitler's operations against Stalingrad and the Caucasus? And, most importantly, among the hundreds of messages they processed per month, did Roessler and Rado's group tell the Russians, in advance, about the German plans for Operation *Citadel*, the vast, and ultimately failed operation that became the Battle of Kursk in 1943? During the winter of 1942, the Germans became aware of the transmissions from the Rado network, and began to take steps against it through their counter-espionage bureaux of the Abwehr. After several attempts to penetrate the network they succeeded in pressuring the Swiss to close it down; this occurred in October 1943 when its radio transmitters were closed down and a number of key operatives were arrested. The Lucy spy ring came to an end in the summer of 1944 when the German members, who were also involved in other anti-Nazi activities, were arrested in the aftermath of the failed July Plot.

The Lucy Ring, Bletchley Park and the Battle of Kursk in 1943

Considerable historical debate turns on what the Lucy Ring did or did not achieve, and whether in fact the German operational plans for the Battle of Kursk were actually betrayed to Moscow by John Cairncross, a Russian-recruited agent working in the section at Bletchley Park that decoded the Luftwaffe's signals, or whether Winston Churchill had wanted Ultra material given to the Russians by covert means.

By February 1943 the Germans had been defeated at Stalingrad, and the Red Army had forced them back across Army Group South's area of operations. The Germans then counter-attacked in March, and established a front line with a 120-mile salient near the city of Kursk, in southern Ukraine. Hitler knew that the Allies would be preparing to invade Sicily or Italy in 1943, and so was aware that he had limited time to make a decisive counter-strike on the Eastern Front: this was designated as Operation *Citadel*, and was planned to break through the Red Army's lines around the Kursk salient. The Germans gathered nearly 800,000 men, 3,000 tanks, and 2,000 aircraft, but were outnumbered by nearly 1.9 million Soviet soldiers, with 5,000 tanks, 25,000 guns and mortars and more than 3,000 aircraft. The Russians had structured a defensive system twelve miles deep, and in some places laid up to 1,500 mines over each mile of front. The two sides could see what the German target was: on 4 July the Germans attacked both sides of the salient in a pincer movement, but despite initial armoured successes, the attack bogged down after three days when the Red Army counter-attacked. Then, on 10 July, the Allies landed in Sicily, and Hitler informed his generals that he was cancelling the offensive and transferring the SS Panzer divisions to Italy, to repel any Allied landings on the Italian peninsula. Kursk was a huge and important defeat for Hitler which, along with Stalingrad and *Bagration*, marked the failure of his campaign in Russia.

Did the Russians know about the planned German offensive in advance? There are three principal theories. The first is that the Allies used the Lucy Ring as a way for MI6 to send military information to Moscow that would not betray the fact that they had broken into the German Enigma system. Harry Hinsley, an official historian for the British Intelligence Services in the war and a Bletchley Park codebreaker, stated that '*there is no truth in the much-publicized claim that the British authorities made use of the* "*Lucy*" *Ring to forward intelligence to Moscow*'.[1]

Britain had been passing Ultra material to the Russians anyway since June 1941, via the British Embassy and Military Mission in Moscow, but this flow dropped to almost negligible levels after summer 1942 when they saw that the Russians were not interested in a reciprocal relationship.

The second theory is the 'unofficial' route from Bletchley Park. From 1942 onwards, the German Wehrmacht High Command had begun to communicate with their Army Group commanders in the field using a machine that the British codenamed 'Tunny'.[†] Colossus, which was the first electronic digital computer that had been pioneered at Bletchley Park, began to decipher Tunny messages from 1943 onwards. John Cairncross, a Scotsman who had studied Modern Languages at Cambridge, had initially been called up to the Royal Armoured Corps, but as a fluent German speaker, he was posted to the Government Code and Cypher School at Bletchley. He worked in Hut 3. Unbeknown to his superiors, he was a Russian agent, one of the so-called 'Cambridge Five'. His codename was *Liszt* because of his love of music. Cairncross smuggled Tunny decrypts out of Hut 3 in his trousers, and put them in his bag at Bletchley station as he travelled to meet his KGB contact in London.

The third theory is that Tunny transcripts decrypted by Colossus were passed to Allied intelligence officers at Bletchley Park, who then created reports based on it, and this material was given to the Russians. Its original source – Ultra – was disguised by claiming that it was routine signals traffic. Many of the original Tunny transcripts were destroyed at the end of the war at Bletchley, but one sole surviving transcript dated from the 25 April 1943, from German Army Group South, signed by Wehrmacht officer Maximilian von Weichs, shows the high level of operational detail available to British intelligence officers. British analysts thus worked out the two German offensive routes, the northern and southern, into the Kursk enclave, and a report based on this transcript was passed through official channels to Stalin.[2] Russian files, however, claim that Cairncross's reports were effective:

> The most valuable 'documentary material about the work of the Germans' in 1943 was the German decrypts supplied by Cairncross from Bletchley Park… the Luftwaffe decrypts provided by Cairncross were of crucial importance in enabling the Red Air Force to launch massive pre-emptive strikes against German airfields which destroyed over 500 enemy aircraft.[3]

Yet in terms of German codebreaking, the spy ring was focal to what would happen to OKW-Chi after the July Plot, and how after this point none of the work of the Third Reich's cryptanalytical agencies was to have almost any strategic or tactical effect, as well as the way in which much of their effective operational lives ended in July 1944.

The SS, Hitler, Reinhard Heydrich, Joachim von Ribbentrop and Himmler had never trusted the codebreakers of OKW-Chi or Pers-Z, and this was the main reason that Göring and the SS had set up their own individual cryptanalytical operations. As we have seen, as early as 1937 Wilhelm Fenner was accused of having anti-National Socialist sympathies. In the wake of the July Plot, after his two senior generals had been executed, a colleague who was a member of the Nazi Party reminded Fenner of a passing comment he had made six years earlier, in which he was denigrating about the SS intelligence agency, the SD. The Third Reich really did try to listen to everything, as Fenner and his colleagues had long known.

Because OKW-Chi was given some of the Abwehr's signals to decrypt, and because the Abwehr and its chief Wilhelm Canaris were suspected of plotting resistance to Hitler, thus OKW-Chi became suspect by extension. Pers-Z had almost ceased to have any tactical or strategic relevance by this point, as firstly, its agency directors were in the habit of falsifying some of the information they learned from decrypted signals, and secondly, because when the intelligence so received actually reached the offices of Von Ribbentrop and Walter Schellenberg, their secretaries would put three-quarters of it into the dustbin, fearing the wrath of their increasingly embittered and paranoid superiors. The strategic effectiveness of the B-Dienst was predominantly halted by the shift in advantage to the Allies, in late 1943 and early 1944, in the Battle of the Atlantic. However, Tranow and his teams came under the protection and leadership of Admiral Karl Dönitz who, as the war progressed towards its ultimate conclusion, came closer to Hitler, and like him became increasingly distracted from any form of operational and strategic reality by dreams of wonder weapons like rockets and giant submarines that would finally win the war for Germany.

So when, in October 1943, the Abwehr sent a message to its headquarters with some potentially explosive information, very little was done about it, and few believed it. The Abwehr bureau in Switzerland received a signal from one of its agents in the United States, an American-Swiss, who worked in the US Navy Department in Washington DC – the agent, stressed the Abwehr, was

their best in North America. The Abwehr report said: 'The English have in their "Intelligence Naval Office" an outstanding aid in the fight against the U-boats.'[4]

As we have seen, Dönitz would order occasional security reviews of the Enigma system after incidents in which it seemed possible that the Allies had compromised it. He did so again after seeing this message, but as the signal did not directly refer to Enigma, and as it originated with the Abwehr and their agent in Zurich, Hans Bernd Gisevius, already suspected of anti-Nazi sympathies, nothing else was done about it. It is possible that the signal originated with the Swiss-American source in the US Navy Department who knew that the British had broken the Swiss Enigma system used to send coded diplomatic signals from Bern to London and Washington, and so assumed in the interests of secrecy and security that they had also broken into the German Enigma, and was making as clear yet strident a warning as he possibly could.

By autumn 1944 it was too late. The final point had been reached: however fast, thoroughly, covertly and well Germany's codebreakers might now gather intelligence from the Allies, it was of little use as the operational ability of the Third Reich to translate it into effective tactical or strategic action was evaporating. The organization and mission of OKW-Chi changed significantly in the summer of 1944, principally because of the attempted assassination of Hitler. Whereas OKW-Chi had supposed jurisdiction over all cipher agencies within the Armed Forces, after summer 1944, it no longer acted like a service agency, but instead set policy and became the primary jurisdiction for all work done on cipher development, message decryption and associated machinery design and construction. The organization changed significantly, with new commanding officers, more focus for the Chi IV function (the codebreaking and translation service) and increased staffing levels. The cryptanalytical departments did their best to try to keep going, but more and more, the German armoured and infantry units out in the mud and on the wire were fighting a battle for their own survival, and no amount of magic in the form of new rockets, brand-new packs of submarines, jet-propelled fighters or stunning codebreaking triumphs was going to help them. Like the Third Reich, they were on their own.

---

* It stands for Glavnoye Razvedyvatel'noye Upravleniye, the Main Intelligence

Directorate.

† The Lorenz SZ-40/42 was a cipher machine that could encrypt teleprinter traffic, and was a more complex and powerful device than the Enigma machine. 'SZ' stood for *Schlüssel-Zusatz*, or 'cipher attachment'. In use from 1941–42 onwards, it was employed by the German Wehrmacht High Command for communications between Berlin and its different Army Groups, as well as Hitler and his generals. Bletchley Park codebreakers who cracked and read into its encoded signals called it and them 'Tunny'.

Chapter Twenty-Three

THE COLLAPSE OF THE THIRD REICH

Major Ferdinand Feichtner described the fighting on Kos and Leros at the end of 1943 as 'the last flare-up of the old German good luck in arms', and shortly afterwards the majority of his Luftwaffe signals intercept units were evacuated from the Aegean islands, and transferred back to Athens, thence to the port of Salonika, and then in a convoy that drove north-west into Yugoslavia, to the town of Pancevo in Serbia, arriving in January 1944. He described a town of Serbian style with no sewage system and no paved streets, but it was the first place his men finally got enough good food. Balkan cooking helped keep his men going as they set up their intercept equipment again. Scanning the skies for Allied bombers and fighter aircraft, his unit sent reports to German fighter command in Romania, Hungary, Greece, Albania and Bulgaria. They benefited greatly from documents captured from enemy aircraft that had been shot down in their area of operations, which showed their radio call-signs. The captured American pilots he found less inclined to tell their German captors very much, as they were well trained in radio security, and displayed a disinclination to talk. Feichtner's rugged sense of military discipline continued as well – in the spring of that year an SS officer sent him a letter, complaining that his son, who was serving in Feichtner's unit, had not yet been made an officer. The Luftwaffe major wrote back to him, explaining the son's weaknesses of character.

When the July Plot took place, Feichtner and his men were taken by

surprise, and shortly afterwards he noticed that the Nazis started to put what he called 'political commissars' into the army at every level. On the Eastern Front, the Red Army moved into Minsk after the overwhelming success of Operation *Bagration*, which had defeated Army Group Centre, pushing the Wehrmacht westwards. Five days after the failed July Plot, the Russians liberated Majdanek concentration camp, and took control of several major Polish towns. By 25 August, the Allies had liberated Paris, while the Red Army was closing in on the Romanian capital, Bucharest.

'Bucharest was a tinderbox at this point,' said Feichtner, 'it was like France but beset by oriental indecency, and the respect that ordinary German soldiers had won was undermined by the foppish and idiotic manifestations [there] of the Nazi Party.'[1]

By the last week of August, Romania imploded, and Feichtner's men had to fight their way out, escaping just before the Red Army moved into the city on 31 August. Again, the men retreated westwards, heading for Graz, in south-eastern Austria. There was little or no time to set up their signals intercept facilities, and the Luftwaffe unit found their reception in the town obstructed by a Nazi Party *Gauleiter*, or administrator, who Feichtner thought 'ghastly', and who wouldn't give the signals men any proper accommodation. 'The young Gauleiter [in Graz] said I could take my soldiers and crawl into the ground, but he came to heel like any other coward.' [2]

The Russians were closing in, and by 1 October there was artillery fire blasting into the crossroads behind the town, just as the autumn rains began. Thousands of refugees, men, women and children, began arriving in the city, ethnic Germans from the Banat region, which sat on the crossroads of Serbia, Hungary and western Romania. Still Feichtner's men retreated westwards, and he arrived back in the Reich for the first time in three-and-a-half years. 'We were now defending our homeland, while I myself lived to the conscientious and disciplined manner of the old Reichswehr soldier.'[3]

The Luftwaffe men lost their out station in the Albanian capital, Tirana, to partisan attacks, shortly before it fell, on 17 November. They then set up another temporary out station in Bosnian territory in Yugoslavia, which held out for six weeks under guerrilla attack. By Christmas 1944, the Russians were beginning the siege of Budapest in Hungary, so Feichtner chose to go and spend the festive season with his men in outlying Hungarian outposts, to try to raise their morale, making sure that at least they had wine and

cigarettes; watching his men enjoy them, their commander noted that it was the finest Christmas memory he had. But American aircraft were now attacking Austria in force, and at the beginning of 1945, the Russians moved into the region of Styria, of which Graz was the capital, so Feichtner and his men moved back towards the state of Upper Austria, and the huge blue lake at Attersee.

As the Third Reich crumbled under attacks from the Allies in the west, and the Russians in the east, with repeated aerial bombing of Germany, Allied leaders met at Yalta in the Crimea. American President Franklin D. Roosevelt, Prime Minister Winston Churchill of Great Britain and Premier Joseph Stalin of the Soviet Union met for a week from 4 February 1945, to discuss the final defeat of Germany and the terms of its post-war occupation. By this time the Americans, British, Canadians and French were advancing into Germany. On the Eastern Front, Red Army Marshal Georgy Zhukov's forces were only forty miles from Berlin, and had taken most of Poland, Bulgaria and Romania. The Germans themselves controlled Norway, parts of the Netherlands, Denmark, all of Austria and much of Germany, the very north of Italy, and the parts of Yugoslavia towards the Austrian border.

At Yalta the Americans most wanted Soviet support in the war against Japan, and wanted the Russians to participate in the United Nations. Churchill was adamant that there should be democratic governments and free elections in the eastern and central European countries, very specifically in Poland. And Stalin? He wanted a Soviet sphere of security and political influence in central and eastern Europe. He also insisted that the demands of the Polish government-in-exile were not negotiable and that the Soviet Union would keep the parts of eastern Poland that they had taken in 1939 under the Ribbentrop–Molotov Agreement. The new Polish government could then extend its western borders into former German territory. Stalin promised free elections in Poland. The future American Secretary of State James F. Byrnes was at the conference; he later said, 'It was not a question of what we would let the Russians do, but what we could get the Russians to do.'[4]

By this late stage of the war, most German codebreaking operations had ceased, as their headquarters in Germany were under constant bombing, or the units – like Feichtner's – were too busy fighting a desperate rearguard retreat back towards Germany. Yet in Budapest, under siege by the Red Army, a small unit of Hungarian military codebreakers still persisted doggedly in trying to intercept Allied and Russian codes.

One SS Sturmbannführer, Urban,[5] acted as the liaison officer between the RSHA and the Hungarian Cryptographic bureau. He worked as an intelligence gatherer and agent handler, and translated into German signals intercepted by the Hungarians, primarily from breaking the Turkish diplomatic codes of their embassies in London, Washington, Paris and Moscow. These were the same codes which the Foreign Office cryptanalysts at Pers-Z had managed to read earlier in the war. Urban's main sources of information were the Hungarians and the Finns, and even by the last year of the war, his allies in Budapest managed to break into between forty and 100 messages a day, with the best information coming from Turkish diplomatic traffic. The Hungarians' 'ace' cryptanalyst was one Lieutenant Titus Vass. In November 1944, as the Russians moved towards Budapest, the entire Hungarian General Staff decided they would move towards Austria, and so their intercept groups and codebreakers came too. Some of their archives came with them, and by March 1945, with part of the journey made by horse and cart, they ended up on the banks of the Danube, in the city of Passau in Bavaria.

The Turkish diplomatic messages which the Hungarians were intercepting contained some of the results of the Yalta Conference. Once they were passed to Sturmbannführer Urban, translated, and forwarded to the RSHA and OKW-Chi, they made their way to Hitler's bunker. They were presented in the form of a memo to the Army High Command, the OKW and the Führer's headquarters. The copy of the memo that was presented to the Command Staff of the Wehrmacht was returned to OKW-Chi. It had notes written on it, which said: '*Dem Hosenscheiszer Kettler sollte man doch endlich das Handwerk legen. Signed Jodl. NB the Führer is of the same opinion signed Fegelein.*' (SS Brigadier Hermann Fegelein worked at Hitler's headquarters as a liaison officer and representative of the SS.) What General Alfred Jodl literally meant was this: 'That trouser-shitter Kettler (referring to Colonel Kettler from OKW-Chi) should stop what he is doing and get another job.' [6]

'*Jemanden das Handwerk legen*' is a German historical term that has its origins in the Middle Ages, meaning to stop someone from doing something, to put an end to something, the word '*Handwerk*' meaning a craft or trade. By now, the Third Reich's fingers were firmly in its ears.[7]

•••

Even at this late hour in the war, Admiral Dönitz was still convinced that new weapons could help win a war that was so obviously lost. The new naval building programme that he had instituted in July 1943 had been designed to construct 2,400 new U-boats by 1948. In February 1945 he announced that a new model of submarine was ready, and he even told Hitler that the new Type XXI 'electro-boats' could travel from Germany to Japan underwater. The first one was only to set sail on 30 April 1945. The new weapons that were supposed to help the Third Reich stave off defeat were being readied too late: when Ferdinand Feichtner attended a conference in March on the development of the Me-262 jet fighter, he compared it to the chaos and collapse around him. He watched Vienna being evacuated as the Russians approached in the first week of April; most of those wearing a German uniform, he saw, had abandoned all sense of honour and duty as a result of years of idleness and self-indulgent excess. The female auxiliaries who had worked for the Luftwaffe signals agency were now being removed from their jobs, pushed out onto the streets without any possessions, terrified like everybody else at the thought of the approaching Red Army. Feichtner put as many of these as he could into his unit's lorries as once more they retreated, this time to Canazei in the Tyrol, where one of his battalions was still holding out and trying to operate, as partisan attacks increased. Old men and teenage boys were forcibly conscripted around the town of Graz, given five bullets each, old Italian rifles, and put under the command of the Nazi Gauleiter who had proved so obstructive to Feichtner earlier that spring. The American army pushed hard into Austria, and suddenly, Feichtner saw that it was all over. The war was lost. The revolutionary weapons like the Me-262 were not going to be the 'magical feat of arms' for the Third Reich that the Nazis dreamed of. On the ground, the hard reality of a lost war rolled towards German units like his, as the tanks and men of the United States steamrolled across Austria. He took his men to Ansbach in Bavaria, to a concentration area set up by the US Army. There, some British RAF officers whom Feichtner described as 'stupefied' captured some of his men, thinking from the first interrogations that they had uncovered an espionage organization. On 1 May came the news that the Führer had killed himself in Berlin and the Russians had taken the German capital. The Luftwaffe major felt the harsh, immediate rush of surrender:

Life was bald and naked in Germany, the Wehrmacht was the

> fountainhead of order, propriety and discipline among the men had been destroyed. The Russians, British, French and Americans took over, but I fear that all Germans who fell into Russian hands are forever lost to any kind of life in a European Community of Nations. For my own part, I hoped to build with my hands a modest existence for myself and immediate family in my own country.[8]

•••

On the Eastern Front, Lieutenant Colonel Hans Eick had watched the German front line crumble and fall back after Operation *Bagration*. He tried to put all of the Luftwaffe's signals intelligence service battalions into one regiment as the Russians pushed forward; by January 1945 he had moved his men and equipment to an area south of Berlin, and then until April they were stationed outside Dresden, half destroyed by Allied air attacks. When Germany surrendered he, like Major Feichtner, moved to a concentration area at Aschbach in Austria. Like so many other German servicemen and women, he was lucky to be alive and lucky to be in the Allied zone of occupation. His last words about the war were that all of the 600 men he had brought with him were accounted for, there was good discipline, nobody had deserted, nobody had to be punished and everybody had enough to eat. It served him, he said, as a bright memory for the future.[9]

Eick's fellow Luftwaffe officer Wadim Herold also retreated west from Russia, and found himself at the same concentration area in Austria as Eick. He felt he had done his duty as a soldier to the Fatherland, had sought no political activity and had been convinced the war against Bolshevism was a necessity. He now had the same urgent concern felt by the German servicemen and civilians whose families were trapped in the areas of Germany and other countries taken by the Red Army; his personal anxiety at the moment, at the end of the war, was for his wife, who was in a region occupied by the Soviet Union. This was a fate shared by Lieutenant Martin Ludwig, who had served in France. After being transferred back to Germany, he too found himself in Austria, but from February 1945 onwards, he had no news of his wife and four children.

•••

After the failure of the plot to kill Hitler on 20 July 1944, Wilhelm Fenner and his colleagues at OKW-Chi found themselves doing battle on two fronts, one far more dangerous than the other. He was still trying to do his job, but his reputation as an anti-Nazi was making things increasingly perilous for him. So was Allied bombing: the office buildings in which he and his team had been working were so damaged by late 1943 that the unit had moved to Halle, and temporarily avoided the difficulties of having to work without rest, at night, in the cold and under regular air attacks. Yet the unit's output only dropped by a quarter or a third. After July 1944 Fenner was accused of being disparaging towards the SS intelligence service years before, which gave rise to a lingering suspicion that he had been somehow involved in the July Plot; Fenner was then accused of trying to sabotage the Reich's cryptographic output by recommending what he called 'inferior' systems, cryptographic processes that did not do their job properly. 'This was due to the ambition of a fanatical party member,' he said. 'But Walter Schellenberg protected me.'[10]

SS Brigadier Walter Schellenberg had by now taken over control of much of the Third Reich's intelligence apparatus; after the July Plot parts of the Abwehr were incorporated into the RSHA, as Himmler and Hitler no longer trusted the Abwehr chief Wilhelm Canaris. Schellenberg was reportedly famous, among other things, for his so-called 'fortress desk', which contained two automatic weapons built into it that could be fired at the touch of a button.[11] 'He protected me,' said Fenner, 'as did General [Fritz] Thiele until he was hanged … they wanted to take Chi, Chi Stelle, B-Dienst, Pers-Z and put them all together under one agency headed by me, excluding Göring's Research Bureau as sure and as certain as the Amen follows the Our Father.'

On 13 April 1945, the Chi staff who did not want to go home travelled on a military train to Werfen on the Salzach River in Austria. Some documents and other material were thrown into the Salzach or burned. On 6 May Fenner, even though nominally a civilian, transferred to the reserves, although Germany was defeated and the war over by this point. By his own account, on the 19th he travelled by train to Landshut in Bavaria, and on 21 May was dismissed from the reserves at Straubing. The Third Reich could no longer listen, but it could still handle its bureaucracy, even in death. Fenner found work as an automobile and bicycle mechanic. His thoughts towards the end of the war were for his son, Siegwart Heinrich, who would have just turned twenty-one that month. He had served as a lieutenant on the staff of one of the units of the Wehrmacht's 'Grossdeutschland' Division; on 19 February

1945 he died of wounds on a hospital train. He was buried in Amberg, Bavaria.

Chapter Twenty-Four

THE MAN WITH THE KEY HAS GONE

The TICOM Investigation

German naval signals intelligence was one of the priority targets for the American and British investigators from the Target Intelligence Committee, or TICOM, as they moved into Germany and Austria in 1945. There were six teams, and No. Six was given the name of Joint Naval Target Reporting Team. They were aiming to cripple German naval signals intelligence by identifying and 'neutralizing' its personnel and equipment. They wanted to discover the exact degree of success had by German naval signals intelligence during the war, through the capture of equipment and the interrogation of personnel. At the outset, they didn't think they would capture any people, but they did think finding equipment was likely. There were six American and British naval officers, all of whom had been through a two-month signals intelligence recognition course. They had two Royal Signals NCOs and two transmitters, while in all thirteen officers were attached to the team during the first days and weeks it accompanied 21st Army Group across north-west Europe.

On 10 April, before they left England, the officers from Team Six had a meeting with Commander Ian Fleming at the London office of the director of naval intelligence, who briefed them on their objectives. They then travelled to Venlo in Holland and linked up with a unit of Royal Marines

from 30 Commando, or 30 Assault Unit (AV), who were to accompany them and provide security for the TICOM team as it tried to capture enemy signals personnel, documents and equipment. Their initial target was the OKM's 4/SKL Group III, the cryptanalytical unit headed by Wilhelm Tranow. They had received reports that in the last days of the war the Germans had developed a coding system called *Flusslauf*, or 'Running River', which was allegedly intended to replace parts of the Enigma coding system.

By 6 May they were in Hamburg, with the war over by only a few days. Germany was in a freefall of bombed-out chaos. Allied units from 21st Army Group were taking control of the north-west of the country, as German units surrendered, were taken captive, held out in desperate rearguard actions, or fled. Team Six reached Neumünster, north of Hamburg, and discovered that on the 4th, the B-Dienst and its personnel had left for Flensburg, further north towards the Danish border. By 7 May the teams had advanced as far forward as Kiel, on the Baltic coast, in area not yet occupied by Allied forces. In the port of Bremerhaven, one team of commandos from 30 AU captured a German destroyer. On the 8th, the TICOM team found encoding tables for the 'Running River' system, which were immediately dispatched back to England. The British and American intelligence officers, with their escort of commandos, moved forward, questioning soldiers, sailors and civilians as they went. On the 17th they hit an intelligence jackpot: they found a whole detachment of naval signals intelligence personnel living in a signals school at one of the B-Dienst's former headquarters at Flensburg-Mürwik, on the Danish border. The TICOM officers decided to interrogate everybody, including an admiral whom they had captured: 'We decided to interrogate everybody, if he [the admiral] proved amenable we would be pleasant and helpful, if he proved obstructive we would be just as unpleasant as him. He was rather scared and very polite, and so were we, and from this meeting the tone was set.'[1]

The intelligence officers and their commando colleagues stayed the night on ships in the harbour; they lunched at torpedo testing stations, and moved fast, questioning all those they thought could direct them towards their targets. On 19 May some of the team's army officers found Colonel Kettler from OKW-Chi: he told them two things. Firstly, where they could find two of their other priority targets, Erich Hüttenhain and Walter Fricke; secondly, he told them about the documents and equipment that had been dumped into the Schliersee. On the 21st they found and interviewed Hüttenhain,

while the team slept on a liner in Flensburg harbour, the *Caribia*, which belonged to the Hamburg-Amerika line.

The town was at this point still the headquarters of what became named 'the Flensburg government'. Just before committing suicide, Hitler had appointed Admiral Karl Dönitz as his successor, who in turn pulled together a small coterie of loyal Nazi officials to form an administration. Formal surrender to the Allies and the Russians was imminent, and the 'government' could do nothing, except try to stall surrender talks for as long as possible so that the maximum number of German service personnel and civilians could flee towards the advancing Allies, rather than the Russians. Formal surrender documents were signed with the Allies and Russians on 7 and 8 May, and an unconditional surrender of all forces under German control took effect from 11.01pm Central European Time on 8 May 1945.

Dönitz was still at his headquarters in the north of Germany, which he had set up in the naval signals school at Mürwik, a suburb of Flensburg. Alongside it were a huge mixture of soldiers, sailors, SS men and civilians who were hiding and taking refuge, hoping desperately that the Allies would arrive before the Russians did. They were lucky. On the 23rd and 24th the British raided the signals school, and a British RAF regiment detachment arrested Dönitz. The TICOM team were able to keep hold of some of their priority targets whom they found in the signals school. One of them was Wilhelm Tranow. 'On the 24th, we interviewed Tranow … after a little prompting to begin with he soon got into his stride.'[2]

Tranow initially said that all material pertaining to the B-Dienst's signals intelligence and cryptanalytical operations had been destroyed, but then gave further details which revealed that in fact some documents had been kept in a bombproof and fireproof safe at one of the B-Dienst's previous headquarters. The following day another officer confessed to having dumped material both in Neumünster and at the town of Torgau, on the Elbe, which was where American and Russian soldiers had first linked up on 25 April.

The interrogation of Wilhelm Tranow by the American and British officers took place simultaneously with four other B-Dienst personnel, two naval officers and two civilians.[3]

'It was actually in 1938 that we broke into British operational systems, the "Cyphers",' he began:

We exploited this practical knowledge at the beginning of the war so

> that we were in a position to read them. At the beginning of the war – I believe 25/8.1939 – all cypher systems changed. At that time our strength was not such that we could work on all the material received. We confined ourselves to the Administrative Code. This was a five-figure code reciphered on a subtractor table. In a short time, about eight days, we had progressed so far as to be able to read it easily again …

Tranow went on to describe the early codebreaking successes of the B-Dienst, the naval cyphers, indicators, personnel shortages, personnel expansion, and the Norway operation.

> In connection with the Norway operation there was practically nothing of importance we could not read … we also read currently the plans in March and during the Norway operation we read everything almost currently.

Reading between the firmly typed lines, Tranow knows this will be the first of several interrogations, and so while he is happy to tell his interviewers what his section achieved, he is correspondingly vague as to how exactly he did it. He triumphs the strokes of good fortune his department had, but then calmly shoots them down:

> We read them [the Naval Cyphers] easily up to the end of December 1941. On, I think, 1/12/1941 we had a 'pinch' of Naval Code from Tobruck. [sic.] We did not get any ciphering tables [*Schlüsselmittel*] only the Code [Book]. Since we had worked this out for ourselves, it was not of importance.

Should his British and American interrogators be in any doubt as to the efficiency and capabilities of his department, he reminds them from time to time:

> In January 1942 there was a complete change in all codes, Naval Cypher and Naval Code. In ten days we had got so far with Naval Code as to be able to read some of it …

Like a capable player playing out a complex hand of bridge, he proceeds through descriptions of codes and their decipherment, and then moves on to

talking about Atlantic convoys.

> Then in October 1941 the Naval Cypher for Anglo-US traffic was introduced. The traffic in this Naval Cypher was at first slight, but we discovered that you (the Allies) were using your old system, the old 5-figure indicator which was in force up to January 1941.

'You mean it was reintroduced?' asks the interviewing officer.

'Yes,' replies Tranow:

> Since we established after a short time that this Code was used for convoy escorts, we turned our special attention to it and in spite of the slight amount of material received we had progressed so far in February/March 1942 that I believe the traffic of every convoy sailing, whether in the North Atlantic or Pacific or South Atlantic, wherever the code was used, could be read. In many cases the convoy schedules could be read in good time.

The interviewer then takes a pencil and marks a line beside the next five lines of typed text, to emphasize their importance:

> In June 1942 the same indicating system as for the other Codes was introduced. This gave us no trouble. We continued to build up the code. We broke the keys to such an extent that in this code we sometimes read 80% of the entire material from mid-1942 onwards until about 15/12/42 …

He explains administrative difficulties and shortage of personnel, but also how his department triumphed over these obstacles: 'We took personnel from active service.'

'Did you always get them or were there difficulties?' asks the interviewing officer.

Tranow replies:

> There were always administrative difficulties. It was not easy to prove to a layman the necessity for employing about 700 people in one particular sphere. We only found understanding for this with one's own Departmental Chief, but it was not easy to find sympathy in the

> administration as the men were needed on active service too. Some of these who had to be withdrawn from the front were specialists. With the advent of the new and briefly trained personnel we again made progress with the deciphering of Naval Code and Naval Cypher USA i.e. of the Convoy Cypher, so that we were frequently able to read all that interested us in the North Atlantic (in which the Western Approaches and Halifax routine telegrams and the 'Convoy Sailing' telegrams from New York were useful to us) so quickly that we often had our information 10–20 hours in advance. Up to the beginning of June 1943 we were well in the picture.

Tranow then proceeds to describe how, after the B-Dienst were bombed out of Berlin, they left behind some of their documents in a bombproof cellar on the Messedamm. This, he said, was near the wireless mast Bretschneiderstrasse 5/7, close to the Witzleben station and Silk Industries House.

'Did you leave the texts of our signals?' asks the interviewing officer.

'No,' replies Tranow cunningly, 'only the important ones.'

As he then describes the perambulative moves of the unit at the end of the war, and its staff which fluctuates at around 250 people, he drops in and out of his answers references to documentary evidence and material that is sometimes destroyed, and then sometimes preserved, with nobody quite sure where it is to be found. Then come the questions as to how he decrypted Allied systems, and Tranow describes the workings of his team, immediately stating that no records remained of how they did this. As the questioning continues on the whereabouts of the B-Dienst's documents and archives, the interviewer keeps returning to the subject. Where are the records? One colleague of Tranow's simply says that not only were all original documents destroyed, but also all and any documents that might have existed in duplicate. Another colleague, a naval captain, simply says that all documents were destroyed, not a single piece of paper was left. Everything was burned. Tranow then details the breaking of Russian codes with Finnish assistance, dallies with Spanish and Italian codes, and the interviewing officer is left knowing very clearly *what* Tranow and his team achieved, but remarkably little on *how* they did it, and if there are or aren't any records at all anywhere that have or haven't been destroyed. Wilhelm Tranow and his team out-fox their interviewer in the first round.

The interviews with Tranow continued, affording the interrogating officers continued descriptions of the B-Dienst's achievements, but little of their methods. On 30 June 1945 both Erich Hüttenhain and Walter Fricke left for England, and further questioning.

•••

Much further south, three other TICOM teams were at work. American and British officers had a target list that included the Japanese ambassador, Oshima, and his fellow diplomats found in the hotel at Bad Gastein; then there was Hitler's headquarters at Berchtesgaden, Göring's train, Von Ribbentrop's villa, an SS headquarters in Bavaria, and the last known halt, on their retreat westwards, of the 350th Luftwaffe Signals Intelligence Regiment near Innsbruck.

As one TICOM officer reported, surprising streaks of bluff and banditry broke the surface in members of the team, serving to overcome all obstacles. The British and American officers were on a freewheeling mission where they had to think on the hoof and take their clues, and their cribs, where they found them. The Japanese diplomats were interned and arrangements were made for them to be transported back to the United States. Wearing a pair of German army officer's jackboots he had looted, one TICOM officer oversaw the search of tunnels below an SS barracks at Obersalzburg, but nothing was found. By now it was 21 May, and still they had found almost nothing. Working parallel to them was another team from TICOM who were about to embark on the search of the lake at Schliersee.*

Then on 22 May they were told by some captured German technicians that they had just finished burying some technical equipment. The TICOM team asked them to unearth it again, and discovered an entire set of machinery for the Russian teleprinter encoding and transmission system that was called Baudot, after Emile Baudot, the man who invented it in 1870. A German team from the army's cryptanalytical section, GdNA, had discovered it in Russia and transported it all the way to southern Bavaria where, for want of something better to do and keen to hide it from the Allies, they dug a series of holes and buried it. It weighed eight tons. The TICOM officers made sure that every single part they could think of was accounted for, and then the heavy pieces of equipment were put onto lorries and taken to be flown to England.

The team then followed up other leads, searching a signals dump in a lunatic asylum, questioning an SS man who claimed to know something about invisible inks, and searching foreign minister Von Ribbentrop's summer house. When the Allied soldiers were loading the eight tons of Baudot equipment onto aircraft at a nearby airstrip, they got lucky again. Directly opposite the entrance to the airfield was a set of six buildings, which they searched. In one building a document was discovered that was a sketched organigramme of Hermann Göring's Research Bureau, the Forschungsamt. They also discovered an officer called Schapper, who said that he had joined the Research Bureau in the 1930s after defecting from OKW-Chi because of the incompetence of their cipher bureau. The officer told the men where they could find the documents and equipment that the bureau had hidden nearby. When they did, they discovered a cache of decryption equipment and decoded signals both from German signals intelligence organizations and from foreign embassies across Europe. These joined the burgeoning haul of material that TICOM was by now gathering, to which would be added the documents and machinery that their fellow team was by now trying to retrieve from the Schliersee.

At Strub in Upper Bavaria they searched the school of the Bund Deutscher Mädel, or League of German Girls, the female youth wing of the Nazi Party. The rooms were bare; there were only some teleprinters stripped of their rotors and wheels. Outside one building the TICOM officers decided to requisition three Mercedes cars, but a German signals officer stopped them, with a document signed both by Field Marshal Kesselring, and by the American 101st Airborne Division, in whose operational area of occupation they were now working. 'The 101st had taken over the area,' said the TICOM team's report, 'but some Germans refused to believe the war was over: they were truculent, and we all got stuck in the middle of a situation, who would shoot us first, the Americans, Germans or TICOM?'

The German officers that TICOM found said they had orders from Allied headquarters in Brussels, transmitted by radio, to stay where they were, so the TICOM team simply escorted them to Strub, where the Germans celebrated so fulsomely that two of their officers had to be taken to hospital with broken legs, and others, said the team's report, remained *sotto blotto* for thirty-six hours and could not be interrogated. Meanwhile the American and British officers from TICOM Team One made one of the most significant discoveries of the early stages of their operation. From 1945 to 1947,

hundreds of interviews would be held with German prisoners, similar to the one described above with Wilhelm Tranow. These could only take place once the TICOM personnel had discovered who exactly it was they were looking for, for which signals intelligence or cryptographic agency they had worked, and what they might know. In those first days of operations in Bavaria, the late spring and early summer of 1945 were only just stretching out their hands and taking hold of the tenuous, war-bruised arm of peace, to see if it had a beating pulse.

On 21 May, three officers from TICOM Team One were at a POW camp set up in the town of Bad Aibling, a spa resort south-east of Munich known for its mud baths, which contained peat pulp. They were looking for German signals intelligence personnel when they were told by some of the other prisoners that one POW knew a great deal about decoding Russian signals traffic; the POW in turn said that he used to work for the GdNA in Russia and knew all about the so-called 'Russian Fish', a type of German wide-band receiver used to intercept Russian teletype signals. It transpired that other members of the unit were at the town of Rosenheim, and the POWs rounded up twelve large and fifty-three small chests, and another fifty-three boxes which all put together weighed seven-and-a-half tons. As the TICOM officers watched, the Germans reassembled the machinery and shortly were able to start intercepting Russian traffic there and then.

The German POWs and all the equipment were taken to the headquarters of the American Seventh Army in Augsburg as plans were made to transport them to Britain. TICOM and the American military interrogated the prisoners, of whom one was called Erich Karrenberg. He was born and educated in Russia and became a lecturer in the History of Art and Music at Berlin University; his Russian language skills saw him working for the GdNA in a wire-tapping unit on the Eastern Front, before being put to work on the 'Fish' device, working out the teletype's daily letter layout. TICOM were to describe him as probably the single best source for TICOM on the details of the Russian 'Fish'. Karrenberg and some other prisoners who had worked for the GdNA, including one who had worked on the NKVD's codes, were taken to England. They reconstructed the 'Fish' apparatus in the gardens of a country house in the village of Steeple Claydon in Buckinghamshire, wiring one of their aerials nearly 100 feet up a tall tree. They began to intercept Russian radio traffic straight away, and this virtuoso intelligence coup by TICOM was only brought to a temporary halt when the local post office sent

a notice complaining that some local residents were upset because their reception of the BBC was adversely affected.

Back in Bavaria, other TICOM officers found their way to Hitler's former residence; it was gutted, but in his personal air-raid shelter they found classical victrola records and gold picture frames, and a large telephone exchange. The actual personal headquarters of Hitler was now the headquarters of the 101st Airborne Division; down under the hill was an air-raid shelter in which they found a list of Hitler's movements, day by day, hour by hour since the 1930s. As spring 1945 turned into summer, the TICOM teams searched and interrogated and chivvied their way across both northern and southern Germany, starting to uncover the enormous technical and personnel infrastructure of the Third Reich's signals intelligence and cryptanalytical capabilities. It was a task that would continue for two years, and result in the enormous archives of material that were to be held by the American National Archives, as well as providing technical information that helped the Allies feel their way into the Cold War. Shortly after leaving Berchtesgaden, two TICOM teams headed back to England by road in commandeered trucks on which they had simply painted American military white stars. Some of the vehicles were driven by German prisoners, and as the convoy passed through one town in Belgium, the local civilian population took offence at the sight of hated Germans at the wheel of American vehicles. Even though peace was now well into its stride, there was a TICOM casualty: an American officer, Lieutenant Levenson, was hit by a tin can hurled by a furious Belgian woman.

---

* The search of the lake at Schliersee is described in the Preface.

EPILOGUE

What Became of the Characters after the War?

Heinz Bonatz
In June 1945, the former head of the B-Dienst was given command of a German naval unit clearing mines in Holland until 1946; released from British custody in August 1946, he later wrote two volumes of history about signals intelligence in both World War I and World War II. He died in 1981 at Witzenhausen, Germany.

Alexis Dettmann
He was in British captivity from January to May 1945, and placed himself at the disposition of the Americans in 1947. He wrote very lengthy reports about the operations of the GdNA in Russia for the Allies between 1945 and 1947. The American officers who interrogated him said that 'on the basis of his long experience and practice in an administrative capacity, but in particular due to his practically uninterrupted employment in all parts of this field, the author is the only person in Germany who is in a position to compose a report on all Russian military and political cryptographic systems with respect to the possibility of decipherment.'

Karl Dönitz
He was sentenced to ten years imprisonment at the Nuremberg trials on charges of war crimes, and after he was released he lived for the rest of his life in a village outside Hamburg, until he died in 1980. Both his sons died in the

war, one in a U-boat, the other on an E-boat that was sunk by a French destroyer.

Ferdinand Feichtner
In the TICOM series' Seabourne Report into the Luftwaffe's signals intelligence service, he was described by the US Air Force authors thus: 'By general acclaim of his fellow officers he is credited with having made the greatest single individual contribution to the development and subsequent success of the SIS of the Luftwaffe.'

Bonner Fellers
Decorated with the Distinguished Service Medal and promoted to brigadier general for his reporting from Africa, he then joined the Office of Strategic Services, or OSS, before serving in Japan. He was the liaison officer between American headquarters and the Imperial Household, and argued strongly that it would not be in the Allies' interests to prosecute the emperor and his family for war crimes. He retired from the army in 1946 and died in 1973.

Wilhelm Fenner
On 2 July 1946, he was arrested in Bavaria where he was repairing bicycles. Ostensibly as a witness needed at Nuremberg, he remained in an Allied prison in Straubing until August 1946, and then was taken for lengthy interrogations by TICOM at Haus Alaska, which was the codename for HQ 7707 European Command Intelligence Center Camp King, the US Army's interrogation centre at Oberursel near Frankfurt.

Walter Fricke
He became the primary witness for TICOM about the running of the Lauf intercept station. Parts of his work are still classified in Germany today.

Erich Hüttenhain
TICOM took him to the United States to be interrogated. He built a machine for them that decrypted the settings of a Russian rotor machine, and on his return to Europe in 1947, he worked for the Gehlen Organization. The Gehlen Organization, or Gehlen Org, was an intelligence agency established in June 1946 by US occupation authorities in the United States Zone of Germany, and consisted of former German army staff officers who had served on the Eastern Front. He then went to work for the German

Central Office for Encryption, the first official cryptographic service of the federal government, where he cooperated with Adolf Paschke, Kurt Selchow, Rudolf Schauffler and Heinz Kuntze, some of the best wartime cryptologists in Germany. One of his objectives was that, unlike in the war, all cryptographic procedures would be incorporated into a single office.

Otto Kretschmer
The legendary submarine commander survived the war, having sunk over 240,000 tons of Allied shipping. He joined the new German navy in 1955, and in 1970 retired as an admiral. On a holiday boating trip in Bavaria in the summer of 1998, he died in an accident on the Danube, while celebrating his fiftieth wedding anniversary at the age of 86. His body was cremated, and, fittingly, his ashes were scattered at sea.

Bruno Kröger
The German who worked hard to break the secrets of the Swiss Enigma offered his services to the American government at the end of the war. It is not recorded whether they accepted.

Wolfgang Martini
The head of the Luftwaffe signals intelligence service, and Ferdinand Feichtner's senior officer, he was detained by the Allies in Germany until 1947 and then released without charge. He worked after the war for the radio firm Lorenz, which had manufactured the machine used by the Germans. In late 1944, fearful that records of wartime radar development would be destroyed or lost after the eventual surrender of Germany, General Martini had key documents buried in a waterproof metal casket. In the early 1950s, Martini recovered the casket from what was then the Soviet-occupied German Democratic Republic. Martini died of a heart attack in 1963, in Düsseldorf.

Arthur Scherbius
The inventor of the Enigma machine died in 1929, crushed during an accident involving a horse and carriage.

Kurt Selchow
After the war he worked for the new German Central Office for Encryption, along with other cryptanalysts from OKW-Chi, Pers-Z and the GdNA.

Wilhelm Tranow
On his release from Allied custody, he worked as an editor at the newly established German national press agency in Hamburg, *dpa*, Deutsche Presse Agentur.

Heinz Walkerling
After the 'greatest convoy battle of all time', Walkerling carried out two more patrols, and then left U-91 under the command of another officer. He had sunk five ships totalling 27,000 tons and spent 156 days at sea. He served with other submarine flotillas and then instructed at the Torpedo School at Flensburg-Mürwik, from September 1944 until the end of the war. He died in 2001.

CONCLUSION

In the early 1920s, the German naval codebreaker Wilhelm Tranow decided that his signals intelligence agency should buy the new Enigma encoding machine. He cannot have foreseen the enormous interest the world would have developed, seventy years later, around cryptography and cryptanalysis in World War II. This book has tried to present just some of the background, operational details and personalities who were involved in German codebreaking, codemaking and signals intelligence both before and during the war. It has attempted to illustrate this story with information, operational examples and personal accounts that are colourful, interesting and accurate. The British historian Sir Max Hastings has researched and written about World War II for forty years and has succinctly summarized one of the main, unanswered questions. 'It remains one of the most fascinating puzzles of the Second World War,' he writes, 'how a society as advanced as Germany failed to match the Allies as codemakers and codebreakers.'

The answer is that it did and it didn't. The Allies' reputation for successful wartime codebreaking is based, to a large extent, on the abundant laurels called the breaking of Enigma, and the resultant haul of Ultra intelligence. And with each book or television documentary or film that appears telling the story of the triumphs of Turing, Hinsley, Tutte, Flowers and Newman, and their determined, intellectually imaginative coterie at Bletchley Park, these laurels are further burnished. And quite rightly so. The scientific triumph not just of breaking the Enigma codes, but continuing to break them for three years, and then keeping it all secret, while benefiting operationally from the resulting intelligence haul, was an astounding achievement and deserves to

have been repeatedly hailed as such. The secrecy aspect alone was astounding. This author's aunt, for instance, waited until she was ninety years old before she confirmed to some of her nephews and nieces that she had worked at the Government Code and Cypher School at Bletchley Park.

But its laurels are composed of many intertwining leaves, of more than just success with the German naval Enigma codes, and the strategic effect that they did or didn't have on the Battle of the Atlantic. There were more than a dozen other Enigma encryptions broken too, such as the Luftwaffe and army codes, and it could be argued that the Allies' knowledge of the army code swung the outcome of the crucial Battle of Kursk in 1943. And then there were the successes with the Lorenz ciphers, not to mention the colossal American contribution to Allied codebreaking. But all of this is largely known, and has been admirably documented since the Enigma secret first became public knowledge in the early 1970s.

However, one of the effects of the telling and re-telling of the Allied success with Enigma, is that it reaffirms in the public imagination a picture of a single-issue problem solved with single-issue application leading to single-issue success. With pluck and valour, the British captured the dastardly Enigma machine, brilliant, undersung and often eccentric scientists then cracked its codes, along the way inventing the computer, and meanwhile U-boats couldn't sink Allied convoys so Britain didn't starve and it was subsequently possible to invade Europe and defeat the Nazis.

Would that things had been so simple.

The enormous and often successful German operations from the early 1930s onwards to break the codes of the British Royal Navy and Merchant Navy have been discussed in depth in this book. What is certain is that the outcome of this battle was the result of many equally strong forces, aside from the decryption of a German communications code, however much of a scientific achievement this codebreaking represented. The United States Navy wrote a confidential report in 1952–53 for the National Security Agency.[1] It analysed and summarized the impact on the Battle of the Atlantic of successful signals decryption of each other's codes by both Germans and Allies. It drew on such detailed documentation as the daily operational war diary kept by the headquarters of the U-boat service, the signals sent by each German submarine, and every Allied convoy report. It states unequivocally that one of the major factors that led to a significant decrease in the tonnage of Allied shipping being sunk by U-boats was the decision made by the Allies

in late spring 1943 – albeit three years too late – to change the codes used by convoys and their escorts. It argues strongly that for a crucial period of the battle – much of the year 1942 – the decryption of Enigma also had no impact on it as the Allies were 'blind' to the German U-boats' communications. David Kahn, the American historian of cryptology, says succinctly that 'the cryptanalysts contributed their part, but no one-to-one correlation existed between them and the sinking rate'.[2]

The British Admiralty went further in their post-war analysis of the impact of German naval codebreaking, published in 1945. So effective were the German cryptanalysts, and so fast, says the report, that between February 1942 and June 1943 (the height of the Battle of the Atlantic) they were reading all the British naval and convoy codes, sometimes twenty hours before a convoy would arrive in a given position. Only after the disastrous losses resulting from the German attacks on the HX-229 and SC-122 convoys in spring 1943 did the Allies conduct a comprehensive security review and change their codes. [3]

Unlike Enigma, German codebreaking wasn't single issue, or single agency, and its successes and failures differed from those of the Allies', but were no less significant. The German codebreaking and signals intelligence operations that prepared them for war in the 1920s and '30s were major triumphs of science, deception, logistics, determination and imagination. The British and Americans concentrated primarily on breaking the codes of two of their enemies – Germany and Japan. The Germans had half the known world arrayed against them, and broke the codes of France, Spain, Switzerland, Russia, Turkey, Italy, Romania, Portugal and Ireland, just to begin with, not to mention British naval and diplomatic codes. And this was before the war had even started. Germany picked itself up from the political and economic doldrums of national bankruptcy in 1920, and created a multi-agency decryption capability that grew and developed at the same speed as radio technology. Before the conflict had even begun Germany was at work intercepting and decrypting and deciphering and reading the signals of fifteen different countries – in fifteen different languages. The Germans then made their signals intelligence agencies applicable to warlike purpose. As late as July 1944, with Allied bombing raids making their daily working life almost unfeasible, the Wehrmacht High Command's cryptanalysts were still deciphering and reading codes and ciphers from thirty-three European and non-European countries. And should there have been any difficulties in

finding or reading or breaking these codes – well then, the Gestapo, along with a sprawling international network of informers, agents, spies and burglars, was on hand to try to get hold of the codebooks, through means sometimes fair, but mostly foul.

But one of the Germans' primary mistakes was a lack of trust between the different codebreaking agencies and their senior German leaders. Whereas British and American codebreaking largely enjoyed unity of purpose, the different German cryptological agencies at best tolerated each other, at worst distrusted the others and sought to demean or defeat their efforts. The decade-long and often lethal feuds between Nazi and anti-National Socialist senior staff members in the Wehrmacht High Command and Foreign Office codebreaking agencies of the Reich is just one illustration of this. Wilhelm Fenner, who ran the High Command agency, remembers the bloody aftermath of the 20 July Plot in 1944. The Gestapo had just arrested two of the most senior Wehrmacht generals responsible for signals intelligence and decryption, and taken them off to be shot or guillotined or strangled with wire, and then be hung from meathooks. Everybody in Fenner's agency was under suspicion. An SS officer told Fenner, darkly, that he remembered an incident from before the war in which Fenner had been overheard making disparaging remarks about the intelligence services of the SS. Such a working atmosphere was not remotely conducive to effective codebreaking. Added to this climate of toxic jealousy and suspicion was the organizational error which meant that six agencies doing the same thing duplicated each other's work.

For as long as the Germans had the naval, military and aerial capacity operationally to implement their successful codebreaking and the resultant intelligence, then the signals intelligence capacity they had worked so hard to build in the 1920s and 1930s contributed directly to their victories. The invasion of France, the Battle of the Atlantic from 1939 until April 1943, North Africa, Kharkov, and the fighting in Sicily and Italy were among these. Crete was a sorry reminder that a country can have dominance of operational power and superb intelligence, but still only narrowly avert defeat. The siege of Malta and the story of the Allied convoys sent to re-supply it were proof that when both sides were simultaneously breaking each other's codes, in the final analysis it came down to who had the better ships and aircraft, with better pilots and crews. *Overlord* and Normandy showed that a nation's armies can possess excellent intelligence, but if the Tiger tanks which are going to implement this knowledge on the battlefield are kept in check by air

attack from RAF Typhoons, or unable to access spare parts and an adequate supply of fuel, then it is worthless.

And the Battle of the Atlantic itself must stand alone as a unique piece of scientific warfare: the Germans were reading British codes, and the British were reading German codes. The former could not believe that Enigma had been compromised because, if it had, then surely the British would have mentioned it in their messages? Wilhelm Tranow, the naval cryptanalyst who had insisted on buying the Enigma machines in 1923 so that the German navy wouldn't have to rely on codebooks, as it had done so disastrously in World War I, now found himself caught by the impressive British ability to keep a secret. This was all the more noteworthy as the Germans often considered the Allies loose-lipped and lax with radio discipline.

Surely, thought the Germans, if the British were reading Enigma, they would have made it apparent in their own signals traffic that they possessed information that could only have come from the decryption of German codes. And since the British didn't appear to know that the Germans were reading some of their naval and diplomatic codes, and since they hadn't made reference to Enigma in their messages, then it stood to sound Teutonic reason they hadn't compromised it. The British, on the other hand, were prepared to admit to a limited audience that the Germans were reading their naval traffic, and were quite willing to admit it to some of the officers of the embattled corvettes and destroyers whose job it was to escort the convoys. The British proved better at keeping the secret of Enigma than hiding the embarrassing truth that their own codes were compromised. The post-war secrecy rules have meant that it has been possible to perpetuate the achievements of Bletchley Park, and leave the telling of significant intelligence shortcomings to the fog of the past.

The German historian Jürgen Rohwer was a prominent naval writer, who served on a Kriegsmarine minesweeper and destroyer in World War II, and then went on to write some 400 books, pamphlets and papers about naval wartime intelligence. He was one of the few people who worked out and knew how Wilhelm Tranow actually read the Allied naval codes. Rohwer died in 2015, but at a lecture in the United States in 1977, he said this: 'Many books, essays and TV shows in recent years suggest that, by using Ultra, the Allied High Command almost always had knowledge of German intentions. If true, this would have led to a much earlier end to the war.' [4]

Rohwer then clarifies the situation, explaining that the Allies knew certain

things that were going to happen in advance. For instance, they knew of the Italian naval movements off Cape Matapan, the intentions of the *Scharnhorst* in the Battle of North Cape, the German plan for Kursk – but such was the fear of compromising the Enigma goose that kept on laying the golden intelligence egg, that they couldn't use it effectively all the time. Secondly, large swathes of the wartime battlefield had to be won by old-fashioned fighting, as in the Pacific, in Italy and Normandy. And sometimes the truth was that the Germans won because they were better soldiers who were better equipped and more experienced. Not all of the time – parts of the British army and their colonial allies were a match for anything the SS or Wehrmacht could field – but significantly often. Thirdly, the answer to Rohwer's question is one not of science but of political economics. America had to beat Japan, and help Britain and its empire defeat Germany in the west, while Russia had to defeat the Third Reich in the east. That was what took the time.

There are conclusive lessons to be drawn from German wartime codebreaking, both strategic and tactical, and hopefully this book goes some way to illustrating these points. Unless a combatant possesses the means to translate good intelligence into operational capability, and subsequent action, the intelligence is useless. An example of this is Operation *Overlord*. If he can do this, the effectiveness of the intelligence depends on the means the enemy has to counter his operational strength, both in hard terms of ships and tanks and men, but also in soft terms of the enemy's own intelligence capability, as in the Battle of the Atlantic. If both sides possess good intelligence and good capability, it doesn't mean the operational result is a foregone conclusion, as was demonstrated by Crete. One side can have exceptional intelligence-gathering capabilities but be let down by a decentralized organization which dilutes this effectiveness. One example was the German decision to split their codebreaking intelligence activities into at least ten large and small agencies. A combatant can have the best intelligence in the world, and the best means to translate it into efficient operational action, but be let down by senior leadership. We need look no further than Adolf Hitler, and the lack of any effective filters between his deranged decision-making and military reality. Codebreaking requires the so-called 'perfect storm' of factors to be present to be able to translate effective signals intelligence and decryption techniques into optimum tactical and strategic results. This happened in North Africa, and in the German decryption and tactical use of the American military

attaché's code. A nation or combatant group can have exceptional codebreaking abilities but if it diverts its successes or capabilities into excessive appraisal or monitoring of itself or one of its sub-divisions, it becomes useless. Lastly, excellent codebreaking and intelligence-gathering techniques are useless if their results are not used, but exist only as an exercise in gathering knowledge. This was the mistake made by the German foreign ministry codebreakers.

The next important question is why the whole story of German codebreaking hasn't been told properly before. The fields of wartime cryptanalysis and cryptography are narrow and specialized, and one of its finer documenters is a particular writer and blogger, who writes Christos' Military and Intelligence Corner. He says, accurately, that much of the material available about German wartime codebreaking has been sitting in American and German archives. It was only in 2000 that the British government returned the 3,900 codebooks, folders of documents, papers and maps from their section of the wartime TICOM archive to the German Ministry of Foreign Affairs. This is material that was captured inside the Third Reich in 1945 by the British and Americans; they added to it by interviewing dozens of captured German signals intelligence and codebreaking personnel. This generated tens of thousands of pages of documents, 29,000 of which alone were only declassified by the American National Security Agency in 2016. And these are archives that need careful examination – a reader can go through dozens of pages about the minutiae of Wehrmacht intercept station administrative setups before a hard, new, sharp and telling fact or detail emerges. One must also bear in mind that the Germans knew why they were being interrogated and were in many cases playing to the gallery. As they sat in an Austrian barn or a Bavarian house, an American intelligence headquarters or a commandeered British boarding-school in summer 1945, being interviewed by an American lieutenant from the Counter Intelligence Corps, or the US Air Force, they would have been playing a careful balancing game in their mind. How much should I tell? Not for nothing had Wilhelm Fenner and his German codebreaking colleagues dumped much of their agencies' documents and technical gadgetry into the dark depths of two Austrian lakes, prior to capture. And when a senior Wehrmacht signals intelligence official said to the Americans that the German army's high command decryption agency had achieved almost nothing of note, he was guilty of supreme dissimulation.

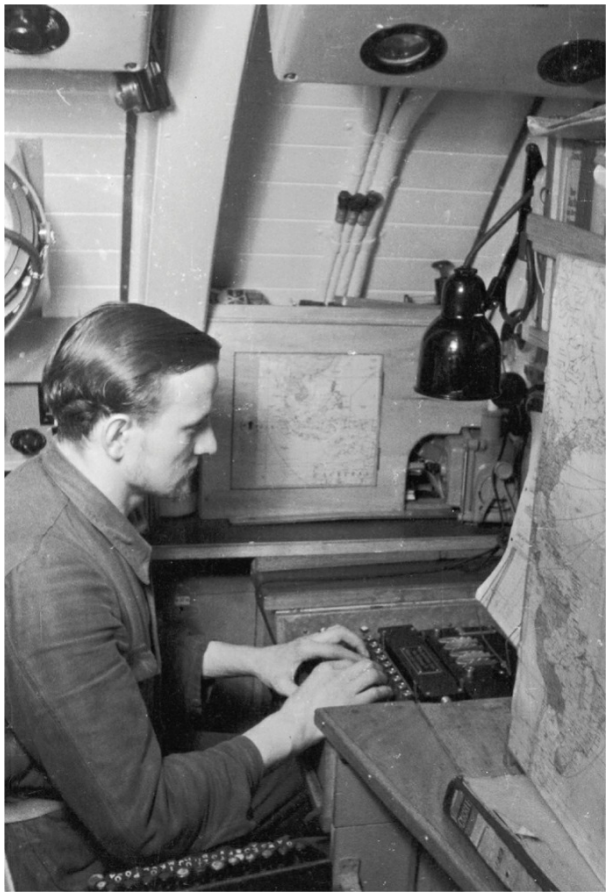
The information about German codebreaking also exists elsewhere. It's in Croatia, Spain, France, Romania, Italy, Russia, Estonia, Britain, Gibraltar and Greece, for example. But even in the face of this geographical spread, much of the verified, opinion-shaping information about codebreaking in the Second World War, in the public domain, in English, is still all about Enigma and Bletchley.

History can be slower to catch up with the world than many imagine. Not everything is findable or recollectable or visible or comprehensible at the click of an internet link, and that is the way that the factual past often prefers to lie. It was only in 1968, for instance, that the British Foreign Office launched an inquiry into German wartime codebreaking, after discovering 100 pages of its confidential diplomatic telegrams sitting in the Ministry of Foreign Affairs in Bonn. The old adage says that there is nothing that can be known that is not already known, but sometimes there can be things that are known but have not been widely seen. Having touched the tip of the iceberg of documentation on wartime German codebreaking, this book tries to illustrate this.

German soldiers in the field enciphering messages on an Enigma machine. (Photo by Time Life Pictures/National Archives/The LIFE Picture Collection/Getty Images)

The Schliersee in Bavaria, where German codebreakers dumped documents and equipment as the war ended. (Photo by Carl Simon/United Archives/UIG via Getty Images)

Luftwaffe signals operators learning Morse code in 1935. (Photo by Willi Ruge/ullstein bild via Getty Images)

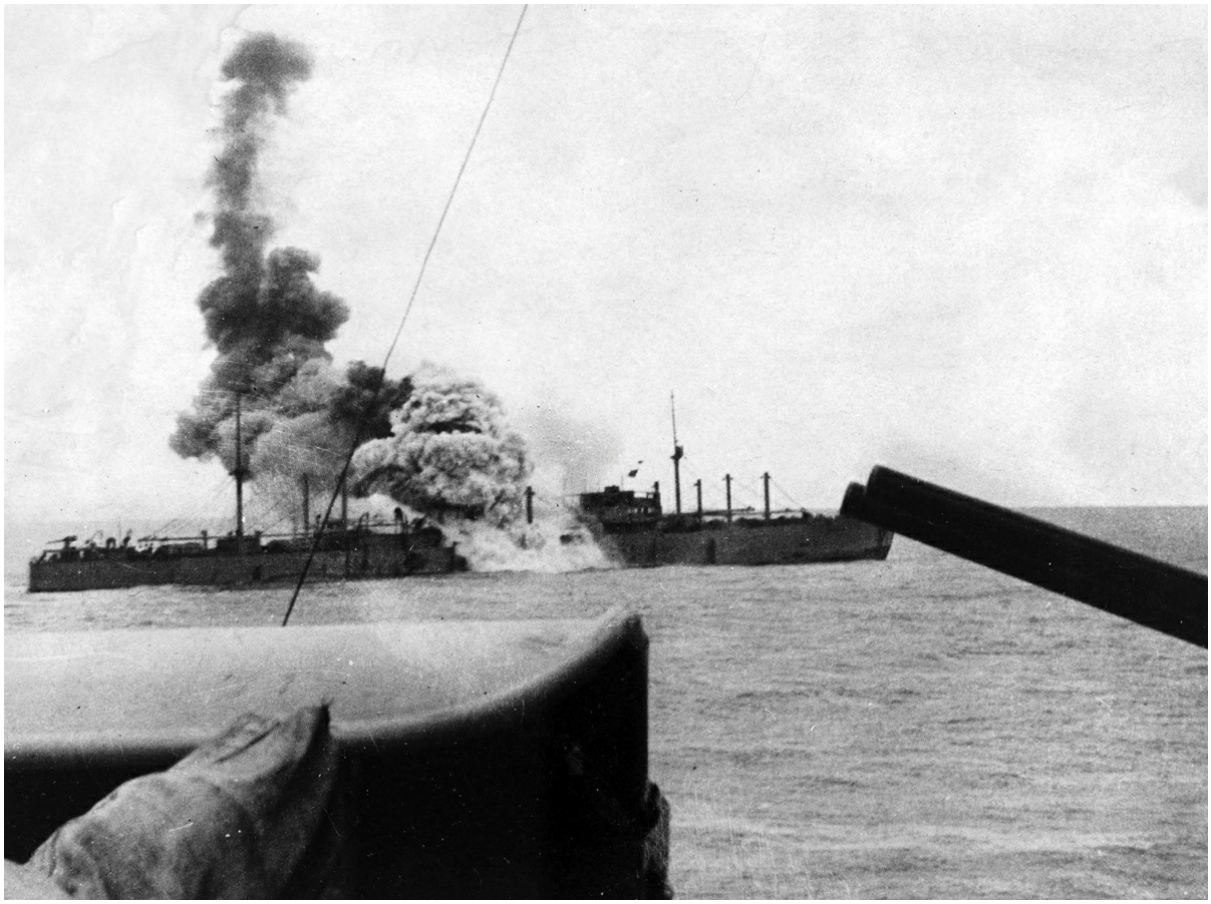


A U-boat radio operator using an Enigma machine. (Photo by Pen and Sword Books/UIG via Getty Images)

During the Spanish Civil War, Luftwaffe personnel from the German Condor Legion helped crack codes used by the Republicans; here troops sunbathe before returning to Germany in 1939. (Photo by Heinrich Hoffmann/ullstein bild via Getty Images)

Survivors from the SS *Athenia* land at Galway in the Republic of Ireland, September 1939. (Photo © Hulton-Deutsch Collection/CORBIS/Corbis via Getty Images)

The P&O Liner SS *Rawalpindi* seen in 1933; converted to an armed merchant cruiser, she was sunk by the *Scharnhorst* in November 1939. (Photo by Topical Press Agency/Hulton Archive/Getty Images)



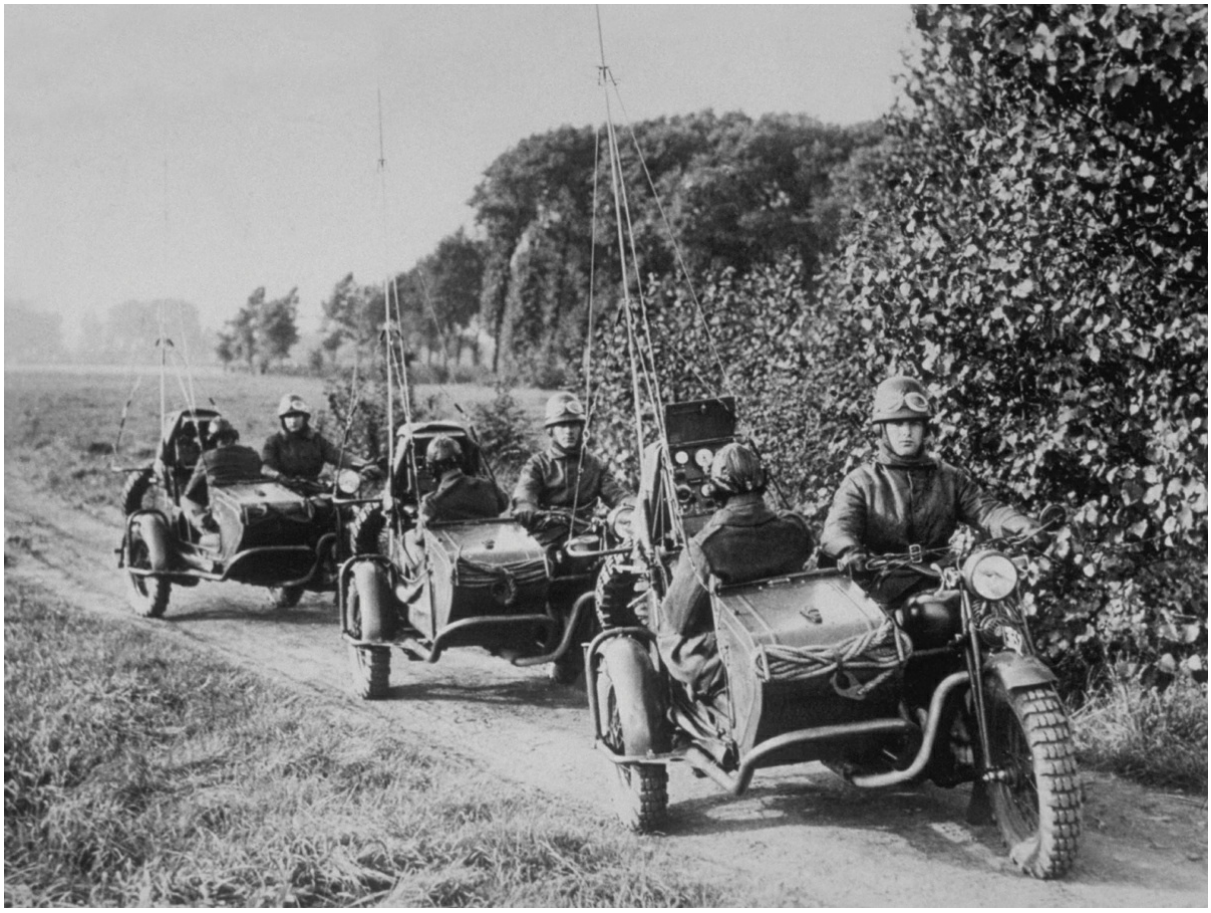
The British merchant vessel *Doric Star* is torpedoed by the German battleship *Graf Spee*; using captured British codebooks, the German radio operators broadcast false messages about their ship's position. (Photo by Popperfoto/Getty Images)

Wehrmacht cryptanalyst and well-known astronomer Dr Walter Fricke. (EN Archive)

Wilhelm Fenner, the cryptographer and administrator in charge of the OKW-Chi codebreaking department. (EN Archive)

Wilhelm Tranow, the B-Dienst cryptanalyst who broke the codes of the Royal Navy. (EN Archive)

Heinz Walkerling, commander of U-91, was heavily involved in the Battle of the Atlantic. (EN Archive)



A detachment of Belgian army signallers on exercise circa 1939. The Germans devised a careful signals deception plan to outwit the Belgians, French and British in 1940. (Photo by Keystone/Getty Images)

German General Heinz Guderian with troops using an Enigma machine during the invasion of France in June 1940. (Photo by Fotosearch/Getty Images)

Luftwaffe cryptanalysts could read some of the RAF's codes, but it made no difference to the outcome of the Battle of Britain; here, German signallers on the ground communicate with planes above them in August 1940. (Photo by Atlantic-Press/ullstein bild via Getty Images)

Admiral Karl Dönitz, head of the German Kriegsmarine. (Photo by Heinrich Hoffmann/The LIFE Picture Collection/Getty Images)

The Germans decrypted crucial signals sent by the American military attaché in Cairo, Bonner Fellers, seen here as a brigadier-general. (US Signal Corps/Bettmann/Getty Images)

Despite good signals intelligence, the Germans struggled to gain an advantage in the first hours of the invasion of Crete. This photograph shows Luftwaffe paratroopers advancing past the bodies of Allied soldiers. (Photo by Keystone/Getty Images)

General Rommel talks to German soldiers during the siege of Tobruk, where a key British codebook was captured. (Photo by Heinrich Hoffmann/Hulton Archive/Getty Images)

The Third Reich is Listening: German personnel during an exam in radio and telephone wiretapping procedures. (Photo by Keystone-France/Gamma-Keystone via Getty Images)

A British merchant seaman covered in oil after his ship was torpedoed in the Atlantic. (Photo by Time Life Pictures/US Navy/The LIFE Picture Collection/Getty Images)

A German U-boat in the Atlantic. (Photo by ullstein bild/ullstein bild via Getty Images)

Fresh provisions stored on a German U-boat at the start of a patrol in the Atlantic. (Photo by ullstein bild/ullstein bild via Getty Images)

British staff encode personal messages to be sent to members of the Merchant Navy. (Photo © Hulton-Deutsch Collection/CORBIS/Corbis via Getty Images)

Luftwaffe signals intelligence teams helped the Germans achieve total air superiority over Sevastopol in 1942: their bombing devastated the city. (Photo by Sovfoto/UIG via Getty Images)

Russian soldiers pictured during the siege of Sevastopol. (Photo © Hulton-Deutsch Collection/CORBIS/Corbis via Getty Images)

German codebreakers succeeded in decrypting signals sent by partisans in the Ukraine. Here, a partisan woman milks a cow to provide fresh supplies. (Photo by Sovfoto/UIG via Getty Images)

German army signallers in Russia in 1941. (Photo by ullstein bild/ullstein bild via Getty Images)

And their opposite numbers from the Red Army. (Photo by Backstein/ullstein bild via Getty Images)

German soldiers in Russia. One Wehrmacht cryptanalyst said ‘the Russians have time, space and winter at their disposal’. (Photo by LAPI/Roger Viollet/Getty Images)

General Erich Fellgiebel, Chief Signals Officer of the German High Command, was executed for his part in the plot to kill Hitler. (Photo by ullstein bild/ullstein bild via Getty Images)

US B-24 Liberator bombers in action over the vital Ploiesti oilfields in Romania, August 1943. Luftwaffe signals intelligence tracked their arrival, alerting flak and fighter crews. (Photo by Hulton Archive/Getty Images)

British troops arrest members of the so-called ‘Dönitz Government’ in Flensburg, May 1945; key German cryptanalysts were also captured. (Photo by Keystone-France/Gamma-Keystone via Getty Images)

Defeat: A wrecked German vehicle and portrait of Adolf Hitler seen in the Dutch town of Groningen, 1 May 1945. (Photo by Keystone/Getty Images)

CHRONOLOGY

2 August 1914: The Russians sink the German light cruiser SMS *Magdeburg* in the Baltic, and recover a copy of the Imperial German Navy SKM codebook; it is passed to the British Admiralty in London.

1915: British troops capture the luggage and equipment of a German explorer and secret agent in Persia called William Wassmuss: they contain a copy of the German diplomatic codebook. Using this, and other cipher books, British cryptanalysts at Room 40 in the British Admiralty intercept and solve an estimated 15,000 German messages between 1914 and 1919.

31 May 1916: The Battle of Jutland; the British Royal Navy's refusal to pay sufficient attention to intelligence received from decryption of German codes denies them a strategic advantage in the battle.

11 January 1917: The German foreign secretary sends the Zimmermann telegram to Mexico, inviting it to join the war on the German side in exchange for territorial gains in the United States should Germany win; the British intercept and decode the telegram, and the US enters the war on the side of the Allies.

1918: A forty-year-old German engineer called Arthur Scherbius from Frankfurt files a patent for a cipher machine; he calls his latest invention 'Enigma'.

June 1919: The signature of the Treaty of Versailles puts a formal end to the war.

Summer 1922: A German journalist and metallurgist called Wilhelm Fenner is put in charge of the German army's new cryptanalysis bureau, along with ten colleagues.

Spring 1923: The German Ministry of Defence puts Captain Walter Lohmann in charge of a programme of covert rearmament in defiance of the Treaty of Versailles, entirely paid for by 'black funds'. The German navy has by now established a new intelligence-gathering bureau, and a former naval radio technician called Wilhelm Tranow is put in charge of cryptanalysis.

1925: A former German army officer called Hans-Thilo Schmidt, now working for the German army's codebreaking bureau, offers to sell information about the new Enigma machine to French military intelligence; they in turn pass it to Polish mathematicians and cryptanalysts also working on Enigma.

15 July 1928: Both the German navy and army decide to adopt the Enigma machine.

1933: Hitler comes to power, and a new cipher bureau is created by Hermann Göring. It is called the Forschungsamt, or Research Bureau. Nazi Party members start leaving the diplomatic, naval and army codebreaking organizations to join it; intense rivalry between the different agencies begins.

1934–37: Wilhelm Tranow and his teams of German naval codebreakers monitor radio signals from the Royal Navy during deployments in the Mediterranean and Atlantic, using these 'cribs' to successfully break into their codes.

1935–38: Tranow's teams begin to read the Navy's Administrative Code in 1935–36, and the Naval Cypher in 1938.

1 January 1937: One of Germany's top cryptanalysts called Ferdinand Voegele is given command of the Luftwaffe's newly created cipher bureau, OKL Chi-Stelle.

Spring 1939: Erich Hüttenhain, a mathematician and Wehrmacht cryptanalyst breaks into the Romanian military and diplomatic codes, enabling the Germans to know what Bucharest will do with its vitally important oil supplies.

July 1939: The Poles, who have now been reading into German signals encrypted on the Enigma machine, give the British and French everything they know.

Summer 1939: Despite staff shortages, Wilhelm Tranow estimates that he and his men are reading the British Royal Navy's Administrative Code, Submarine Code, Auxiliary Code and the principal Naval Cypher about

35–40 per cent of the time.

1 September 1939: War breaks out, and the Germans' partial cracking of the Royal Navy's codes means that on 11 September they can find, and then attack, a British merchant convoy even as it forms up.

October 1939: The German Luftwaffe recover British Syko 'cards' (used by the RAF on an encryption machine) from a Wellington bomber shot down over Germany; the Germans then break into the four-figure RAF and Bomber Command Code.

12 February 1940: German submarine U-33 is sailing off the west coast of Scotland when HMS *Gleaner* depth-charges her; the British capture key rotors from the vessel's Enigma.

April 1940: Erich Hüttenhain reads into the French Ministry of Defence code. Simultaneously, the Italian navy under senior cryptanalyst Admiral Luigi Donini are reading parts of the British Royal Navy's traffic. Wilhelm Tranow's men start to reconstruct the new Royal Naval code, Naval Cypher No. 2, introduced to replace Cypher No. 1 which Tranow has already broken.

Spring 1940: The Germans read the RAF's four-figure code, but it gives them no tactical or strategic advantage in the Battle of Britain.

May 1940: British troops evacuate Bergen in Norway, leaving behind vital codebooks which are captured by the Germans: these include the Royal Navy's Administrative Code, a copy of the Foreign Office Interdepartmental Cypher No. 1, and the current Merchant Ships Code with recoding tables.

22 June 1940: The French government accept an armistice that amounts to a surrender.

July–October 1940: Successes by German U-boats in the Atlantic against Allied shipping lead submarine commanders to dub this 'the First Happy Time'.

July 1940 onwards: U-boats now have bases directly on the Atlantic, on the west coast of France.

1941: Wilhelm Tranow starts to assign British codes with nicknames, based on German cities. German codebreakers from the Luftwaffe, Wehrmacht and foreign ministry break into Swiss Enigma.

January 1941: British codebreakers at Bletchley Park break the Luftwaffe key for North Africa.

4 March 1941: British commandos raid the Lofoten Islands off Norway, and

from the fishing trawler *Krebs* recover two Enigma rotor wheels, the key tables for February 1941 and the plugboard setting.

March 1941: Intelligence gathered from intercepts of Italian Enigma gives the Royal Navy a key advantage at the Battle of Cape Matapan: three Italian heavy cruisers are sunk.

30 April 1941: The fall of Athens to the Germans marks the end of the invasion of Europe.

9 May 1941: U-110 is damaged and boarded off Iceland; a British boarding party recovers the submarine's naval Enigma with its rotors and the key settings for June.

May 1941: German naval divers recover three copies of the Royal Navy's Cypher No. 2, from the cruiser HMS *York* which has been hit by Italian midget submarines off Crete on 26 March 1941.

22 June 1941: Operation *Barbarossa*, the German invasion of the Soviet Union, begins.

11 July 1941: The German commerce raider *Atlantis* opens fire on the passenger liner *City of Baghdad* in the Indian Ocean, and a boarding party discover a copy of the codebook titled *Broadcasting for Allied Merchant Ships*.

Summer 1941: The German navy's codebreakers are reading the British Combined Naval Cypher No. 3, which the Admiralty had introduced on 20 January 1941. The codebook, a four-figure encryption enciphered on a subtractor table, was designed for both the British and Americans to communicate with Atlantic convoys. Tranow and his men codename it 'Frankfurt'.

September 1941: The head of Italy's military intelligence service decides to burgle the American Embassy in Rome and steal and photograph the diplomatic codebook used by the US military attaché for communications with Washington.

October 1941: German army and air force signals intelligence have by now broken sixty-nine different Russian cipher mechanisms, including one code used by the Red Army's General Staff. The Russian five-figure system is called OK40, or Operational Code 40.

February 1942: Intensely concerned that the Allies must be trying to break into their cryptosystems as well, especially given the hugely increased volume of signals being transmitted during the Battle of the Atlantic, the Germans add a fourth rotor onto their naval Enigma, meaning British

cryptanalysts are now 'blind' to the U-boat code called 'Triton', which the British call 'Shark'. Sinkings of merchant vessels from June to December 1942 are now quadruple those from the same period a year earlier.

February–March 1942: The Germans can read, almost daily, the British Admiralty's daily U-boat disposition signal, often on the same night it is produced. This is the intelligence the navy sends to its escort ships and convoys warning of the precise whereabouts of German submarines in the Atlantic.

April 1942: The Germans reconstruct and read the entirety of the British and Allied Merchant Ships Code (BAMS), helped by the codebooks captured by the *Atlantis*. This enables them to read the make-up of convoys crossing the Atlantic before they have left port in America or Britain.

February–June 1942: Luftwaffe codebreakers and signals intelligence teams play a crucial role in Operation *Störfang*, or *Sturgeon Catch*; this is the siege of Sevastopol.

April 1942: The Luftwaffe signals intelligence units in France have reconstructed the entire order of battle, or ORBAT, of the RAF in southern England.

Mid-1942: The Allies estimate they need more than a million tons of imported supplies per week to be able to sustain their war effort, and to ensure the survival of Great Britain.

August 1942: Operation *Jubilee*, the Allied amphibious raid on Dieppe.

30 October 1942: U-559 is sunk with depth charges off Port Said in the Mediterranean, but not before three British sailors from HMS *Petard* manage to rescue the submarine's Enigma key setting sheets with all current settings for the German naval Enigma.

March 1943: German U-boats sink twenty-two merchant ships in attacks on two Atlantic convoys, HX-229 and SC-122. They call it 'the greatest convoy battle of all time'.

June 1943: The Royal Navy change their codes for the fourth time, after a lengthy enquiry into the attacks on HX-229 and SC-122. The German codebreakers can now no longer read their signals and the advantage in the Battle of the Atlantic moves to the Allies.

June 1943: The failure of the German armoured offensive at Kursk in the southern Ukraine sees a major defeat for Army Group South: their retreat from Russia begins.

July 1943: The Allies invade Sicily.

August 1943: The Allies launch Operation *Tidal Wave*, deploying five separate American bomber groups to attack the Ploiesti oil fields in Romania; Luftwaffe cryptanalysts and signals intercept teams track them from their point of take-off in North Africa, and on reaching Romanian airspace German fighters and flak shoot down fifty-three American B-24 Liberators, killing 600 crewmen. The mission is a failure.

October 1943: A Swiss-American intelligence source in the US Department of the Navy sends Swiss intelligence in Bern a signal warning that the Allies have compromised Enigma; the Swiss pass it to the German Abwehr, but no action is taken.

6 June 1944: Operation *Overlord* begins; despite extensive signals intelligence by the Luftwaffe, the Germans have no specific information as to where the invasion will come.

23 June 1944: Operation *Bagration* begins. The Red Army's biggest offensive of the war attacks the German Army Group Centre across central Byelorussia; within days the Wehrmacht is retreating as their central front collapses, resulting in the German army's biggest defeat in World War II. The Russians push into Poland and the Baltic States.

July 1944: Admiral Dönitz's U-boat campaign in the Atlantic officially ends, as all fourteen of the Kriegsmarine's huge 'milk cow' supply submarines have been sunk. German naval codebreakers from the B-Dienst continue to monitor Allied naval activity from their headquarters at Flensburg-Mürwik on the Baltic.

20 July 1944: Plotted, planned and planted by a cadre of senior German officers opposed to Hitler, a bomb explodes at the Wolf's Lair HQ in East Prussia: Hitler escapes with minor injuries. Nearly 7,000 servicemen and civilians suspected of collusion in the plot are hunted down and either executed or imprisoned. The OKW-Chi codebreakers find themselves suspect.

20 August 1944: British, Canadian, American, Polish and Indian divisions begin the huge Allied assault on the German defensive positions stretching across north-central Italy, known as the Gothic Line.

October 1944: Luftwaffe signals intelligence units that have been manning radio intercept and monitoring stations, as well as cryptography units, start to withdraw from the eastern Mediterranean, Albania and the Aegean islands, back to the Balkans and thence Austria.

February 1945: The three Allied leaders, Churchill, Roosevelt and Stalin,

meet at Yalta in the Crimea to discuss the post-war occupation and division of Germany. Unbeknown to them, Turkish intelligence is monitoring the Russian signals from the conference, who are in turn being monitored and decrypted by Hungarian military intelligence, who in turn are giving their information to an SS liaison officer. By the time the decrypted signals from Yalta finally reach Hitler, his chief of staff, General Alfred Jodl, simply refuses to believe them.

30 April 1945: Hitler commits suicide in Berlin, and on 1 May the war ends, with formal surrender signed on 7 May. Allied TICOM intelligence teams move into Germany and Austria, and between April and September, capture both personnel and equipment from Germany's signals intelligence and cryptanalytical infrastructure, including senior officials from the army, navy, air force, foreign office, SS and army headquarters agencies.

BIBLIOGRAPHY AND SOURCING

Several books, articles, websites and blogs warrant mentioning and the author is grateful to the expertise of their various authors during the writing of this book.

For the sheer hard work, diligence, attention to detail and mastery of subject in providing a definitive historical recording and account of one of the largest intelligence coups of the twentieth century, the American National Security Agency's TICOM archive, its archivists, its documenters, its interrogators, its collators, its intelligence analysts, its clerks, its typists and its guardians since 1945 take some beating. Thanks obviously must go to those over the years at the National Security Agency (NSA), at Great Britain's National Archives, Germany's Foreign Ministry Political Affairs Department and others who have worked hard to keep this material extant, and now, over the last decade, to be releasing it into the public domain. One day soon, hopefully, the definitive account of the archive will be written, once the thousands and thousands of pages are declassified and released: the material and stories told in this book are but a tiny part of a vast, fascinating whole.

Two people, as much as any others, have worked hard to present this material in the public domain, to document its declassification, and almost as vitally, to explain it to general readers, and to put it into a format that is not just in scientific and political context, but is at the centre of a crossover between cryptography and history. One of these is Randy Rezabek in the United States, whose TICOM archive website is a superb source of information for those interested in the subject. Secondly, when it comes to documenting and explaining military cryptography, especially from World

War II, the blog and website written at Christos' Military and Intelligence Corner is simply second to none. It explains simply because it understands well. In the endnotes of this book, documents that originated with the TICOM archive are identified by their document number. Some of these were the work of the TICOM teams themselves, while others were put together by the US Army Security Agency, for instance, or the US Navy. The stalwart library and archive staff at the NSA continue to declassify material on an almost weekly basis, and the above-mentioned websites are normally the first to publish the material once it arrives in the public domain; thence it flows outwards towards specialist blogs and magazines.

In 2013, John Jackson, a British writer who works at the Bletchley Park Research Centre, edited *Hitler's Codebreakers: German Signals Intelligence in World War 2.* (BookTower Publishing, UK, 2013). A first and admirable summary of a part of the TICOM documents, it concentrates on around 1,000 pages of material that had then been declassified.

Then come mainstream books. A former World War II intelligence officer, Patrick Beesly's *Very Special Intelligence* (Hamish Hamilton, London, 1977) gives an excellent account of the workings of the British Naval Operational Intelligence Centre in World War II. American historian David Kahn's *The Codebreakers – the Story of Secret Writing* (Macmillan, New York, 1967) is one of the definitive histories of the subject, while Stephen Budiansky's *Battle of Wits: The Complete Story of Codebreaking in World War 2* (Free Press, New York, 2000) is as well-written a book about the interface between science, cryptanalysis and war as there is. Sir John Keegan's *Intelligence in War: Knowledge of the Enemy from Napoleon to al-Qaeda* (Pimlico, London, 2003) is another solid study.

Hugh Sebag-Montefiore's book *Enigma: The Battle for the Code* (Cassell, London, 2004) is the most thorough and best-written of the British accounts to crack the German enciperment on Enigma machines. For one of the best explanatory works about U-boat warfare there is, as well as one fabulous piece of naval history, two books by German naval historian Jürgen Rohwer must stand out. They are *Chronology of the War at Sea, 1939–1945: The Naval History of World War Two* (US Naval Institute Press, Annapolis, Maryland, 2005), and *The Critical Convoy Battles of 1943: the Battle for HX-229 and SC-122* (US Naval Institute, Annapolis, Maryland, 1977).

Mention must be made as well of former codebreaker Harry Hinsley's multi-volume work, *British Intelligence in the Second World War* (Stationery

Office Books, 1979, Cambridge University Press, Cambridge, 1993), Michael Smith's *The Bletchley Park Codebreakers* (Biteback Publishing, London, 2011) which is an updated and extended version of *Action This Day: From the Breaking of the Enigma Code to the Birth of the Modern Computer,* (Bantam Press, London, 2001). Then there is Christopher Andrew and Vasili Mitrokhin's *The Mitrokhin Archive: the KGB in Europe and the West* (Penguin Books, London, 2000). In German, Friedrich L. Bauer's book *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie* (3 editions, Springer, Heidelberg, 2000) and other writings help explain how German cryptanalysts broke into a variety of the codes of their European enemies and allies in World War II.

Among many other sources, the Imperial War Museum in London, the United States Navy Museum, the United States Naval Historical Centre, the IRSML archive and museum in Trieste, Italy, the museum and website of the Italian Navy, the *Regia Marina* in Rome, the websites uboat.net and convoyweb.org, *Cryptologia* Magazine and its website, and the libraries of both the Central Intelligence Agency in Washington DC, and the Technical University of Berlin must also be given mention.

So many books have been written about the Second World War, but as an author who has been reading them since childhood, and is still struggling to understand the enormity of the topic, five authors in particular must stand out for their empirical and consistently engaging coverage of the subject. They are Cornelius Ryan, Carlo D'Este, Sir Max Hastings, Sir Antony Beevor and Rick Atkinson.

GLOSSARY

Abwehr: the counter-intelligence service of the German Armed Forces High Command

B-Dienst: the Beobachtungsdienst, or observation service, the naval intelligence service of the Third Reich

BdU: Befehlshaber der Unterseeboote, headquarters of the U-boat service

COMINCH: Commander-in-Chief of the US Fleet

Deutsche Reichspost: the German Post Office

FAK: an abbreviation of Nachrichten-Fernaufklärungs-Kompanie, a German army signals intercept company

Forschungsamt: the Research Office, a separate cryptological bureau run by Göring

GRU: Glavnoye Razvedyvatel'noye Upravleniye, the Soviet Main Intelligence Directorate

HVB: *Handelsverkehrsbuch*, the codebook which contained the codes for the signals used by the Imperial German merchant fleet

Kaiserliche Marine: the term for the Imperial German Navy during World War I

KONA: Kommandeur der Nachrichtenaufklärung, a signals intelligence regiment in the German army during World War II

Kriegsmarine: German navy from 1935 to 1945

LRDG: Long Range Desert Group, part of British special forces

MTB: motor torpedo boat

'N': Nachrichtenabteilung, or 'news' department, the intelligence division/service of the German Imperial Navy

NCO: non-commissioned officer

NKVD: Narodnyi Komissariat Vnutrennikh Del, or People's Commissariat for Internal Affairs, the Soviet Union's interior ministry

NSDAP: National Socialist German Workers' Party, the Nazi Party

OKH: Oberkommando des Heeres, the German Army High Command

OKH-GdNA: Oberkommando des Heeres/General der Nachrichtenaufklärung, the signals intelligence agency of the German army before and during World War II

OKL: Oberkommando der Luftwaffe, the German Air Force High Command

OKL Luftnachrichtenabteilung: the Luftwaffe's signals agency

OKW: Oberkommando der Wehrmacht, the High Command of the German forces

OKW-Chi: OKW-Chiffrierabteilung, the decryption department of the High Command of the German forces

Pers-Z: Personalabteilung-Z of the Auslandsamt, or Department Z of the German foreign service

POW: prisoner-of-war

RAF: Royal Air Force

Regia Marina: the Italian navy

Reichsmarine: the term for the German navy at the start of the Third Reich; renamed the Kriegsmarine in 1935

Reichswehr: the name of the German armed forces from 1921 to 1935

RKKA: Red Worker and Peasant Army, commonly shortened to 'Red Army' (Soviet)

RSHA: Reichssicherheitshauptamt, or Reich Security Main Office, the security apparatus of the Third Reich

SAS: Special Air Service, part of British special forces

SD: Sicherheitsdienst, the intelligence service of the SS

SIM: Servizio Informazioni Militari, the Italian army intelligence agency

SIS: Servizio Informazioni Speciali della Regia Marina, the Italian naval intelligence agency

SKM: *Signalbuch der Kaiserlichen Marine*, the codebook used by the Imperial German Navy

SS: Schutzstaffel, or 'Protection Squadron', one of the main security bodies of the Third Reich; it was divided into two constituent parts, the Allgemeine-SS, or General SS, and the Waffen-SS, its armed units

TICOM: Target Intelligence Committee
USAAF: United States Army Air force
VB: *Verkehrsbuch*, the codebook normally used by flag officers of the Imperial German Navy
VHF: Very High Frequency
Wehrmacht: the name given to the German armed forces from 1935; it comprised the army (Heer), navy (Kriegsmarine) and air force (Luftwaffe)

ENDNOTES

1. Losing the Signals Intelligence Battle in World War I

1 *The World Crisis 1911–1918* by Winston S Churchill, First Free Press, New York, 2005, Chapter XVI, p. 251.

2 David Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, New York, 1968. *The Daring Deep Sea Divers who helped crack WW1 German codes, by Joseph A. Williams, April 5th 2018*, on www.history.com, gives further details on these conditions faced by the Royal Navy divers. Joseph A. Williams is the author of *The Sunken Gold: A Story of World War I Espionage and the Greatest Treasure Salvage in History*, Chicago Review Press, Chicago, 2017.

3 Quoted in Joachim von zur Gathen, *CryptoSchool*, Springer-Verlag, Berlin, 2015.

4 *Memorandum to the First Lord of the Admiralty on Submarine Warfare*, 29 October 1916, by John Jellicoe, 1st Earl Jellicoe, as quoted in *War Memoirs of David Lloyd George*, Volume 1, Odhams Press, London, 1938.

5 Zimmermann Telegram, 1917; Decimal File, 1910-1929, 862.20212/82A (1910-1929), and Decoded Zimmermann Telegram, 1917; Decimal File, 1910-1929, 862.20212/69, General Records of the Department of State; Record Group 59; National Archives of the United States.

2. The Enigma Salesman

1 David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1933–1945*, Pen & Sword, Barnsley, UK, 2017, p. 33.

2 *The Story of Helmut Ruge of the Graf Spee, Part 1, Germany 1917–1939*, pp. 2–7, www.ww2pacific.com/ruge

3 Admiral of the Fleet, Lord Fisher, *Memories*, Hodder & Stoughton, London, 1919.

4 One of several comprehensive accounts of the Lohmann Affair can be found at the CIA's Online Library: Center for the Study of Intelligence, Studies Archive Indexes, Volume 14 No. 2, 'The Lohmann Affair'.

3. Germany's New Codebreakers

1 TICOM DF-187: *The Career of Wilhelm Fenner with Special Regard to His Activity in the Field of Cryptography and Cryptanalysis.* The information on Wilhelm Fenner's wartime career and cryptanalytical achievements is drawn from a variety of American and British intelligence reports from the period 1945–49. This one is a US Army Security Agency report, numbered DF-187, from December 1949, in which Fenner describes his career. From this point onwards TICOM and Army Security Agency reports are given a number in endnotes, and a page number if and where applicable and available. TICOM archive documents appear in the endnotes as TICOM and are followed by the document registration number.

2 CIA Online Library, 'The Lohmann Affair'.

3 Ibid.

4 Władysław Kozaczuk, *Enigma: How the German Machine Cipher was Broken, and How it was Read by the Allies in World War Two*, 1984, edited and translated by Christopher Kasparek, University Publications of America, Frederick, Maryland, 1984. It is a revised and augmented translation of *W kręgu enigmy, Warsaw, Książka i Wiedza,* 1979, supplemented with appendices by Marian Rejewski. The information above is compiled from the following: Rejewski Appendix A 1984, pp. 246–7; Appendix B to Kozaczuk 1984, pp. 229–40; Appendix C to Kozaczuk 1984, pp. 241–5; Appendix D to Kozaczuk 1984, pp. 246–71; Appendix E to Kozaczuk 1984, pp. 272–91.

4. Preparing for War

1 TICOM DF-187-A, subsidiary to DF-187 quoted above.

2 TICOM-1-201: *The Interrogation of Dr Franz Weisser,* carried out by Lieutenant Mary C. Lane, US Army Security Agency, Augsburg, Germany, 17–18 October 1946.

3 TICOM IF-179: *Volume IV Part 1 of the Seabourne Report, The Luftwaffe's Signals Intelligence Service, Biographies of Contributors – Major Ferdinand Feichtner.* This is a 1,150-page report into the signals intelligence service of the Luftwaffe

compiled by Colonel J.G. Seabourne of the Air Corps of the USAAF in November 1945.

4 Extract from the minutes of the meeting between Hitler and Chamberlain at Berchtesgaden, 15 September 1938, held in the British National Archives, London, file number FO 371/21738.

5 *European Axis Signal Intelligence in World War II*, National Security Agency/Army Security Agency, nine volumes, Nimble Books, Ann Arbor, Michigan, 2010, Volumes 1 and 7; this is from Volume 1, p. 21.

6 HQ USFET Weekly Intelligence Summary no. 12, 4 October 1945 / TICOM DF-241: *The Forschungsamt – Part IV*, p. 40.

7 F. H. Hinsley et al., *British Intelligence in the Second World War: its Influence on Strategy and Operations*, five volumes, HMSO, London; Volume 2, pub. 1981, p. 642.

5. The Kriegsmarine Starts Listening

1 Admiral Luigi Donini, *I Servizi Crittografici delle Marine Britannica e Italiana* (trans. The Cryptographic Services of the Italian and British Navies), Revista Marittima, Gennaio 1983.

6. Two Navies at the Outbreak of War

1 Roy Leadbetter, *My Night to Remember – Sinking of the Rawalpindi*, BBC-WW2 People's War, 15 October 2014, Article ID A1984160.

2 Ibid.

3 Ibid.

4 The detail on the last voyage of the SS *Doric Star* comes from the website of the Blue Star Line, bluestarline.org, and the book *Blue Star Line at War: 1939–1945*, W. Foulsham & Co, London, 1973; the author's name is a pseudonym 'Taffrail', referring to part of a ship's fittings.

5 Dispatch submitted to the Lords Commissioners of the Admiralty on 30 December 1939 by Rear Admiral H. H. Harwood, KCB, OBE, Rear Admiral Commanding South American Division. Recorded in *The London Gazette*, issue 37989, 17 June 1947.

6 Jonathan Dimbleby, *The Battle of the Atlantic: How the Allies Won the War*, Viking Publishers, London, 2015, p.46.

7 *The story of Helmut Ruge of the Graf Spee, Part 2, The Graf Spee,* pp. 8–9, www.ww2.pacific.com/ruge

7. Romanian Codes and Romanian Oil

1 The technical description of the breaking of the Romanian military attaché's code in Paris, written in German, is from Friedrich Bauer, 'Entzifferung 1939–1945', *Informatik-Spektrum* 2008, Bd. 31, Nr. 3, S., pp. 249–61, reproduced with the kind permission of the Library of the Technical University of Berlin.

2 *TIME*, 'Foreign News: Killing', 3 April 1939.

8. Signals Intelligence and the Invasion of Europe

1 TICOM IF-175, which is Volume XIII of the Seabourne Report, referenced previously. Details of the career of Ferdinand Voegele, Chief of Referat E of the Chi-Stelle of the OKL, are to be found on pages 1–28. Voegele appears at much greater length in subsequent chapters.

2 The technical description of the breaking of the French war ministry's code in Paris, written in German, is from Friedrich Bauer, 'Entzifferung 1939–1945'. Parts of it also appear in TICOM I-128: 'Deciphering Achievements of In 7/VI and OKW/Chi', p. 2.

3 TICOM DF-187B: *The Cryptanalytic Successes of OKW-Chi after 1938.* Written by Wilhelm Fenner during his period of detention from September–December 1946 at the US European Command Intelligence Centre at Oberursel, Germany.

4 TICOM I-68: *Consolidated Report Based on Two Interrogations of Oberst Randewig*, pp. 1–7. Compiled from interviews that took place with American intelligence officers on 1 and 10 August 1945.

9. Fighting the War in the Air

1 TICOM I-119: *Further Interrogation of Reg.Rat Voegele and Major Feichtner on G.A.F. Sigint.*

2 This is a description invented and used by the writer Stephen Budiansky in *Battle of Wits: The Complete Story of Codebreaking World War II*, p.135, Simon and Schuster, New York, 2000.

3 TICOM I-201: *Interrogation of Franz Weisser*, p. 6; TICOM IF-178: *The Seabourne Report Vol II Part 1, The Signals Intelligence Service of the German Luftwaffe, Biographies of Contributors: Captain Erich Hubner*. His entry is pp. 30–42.

4 Ibid.

5 TICOM I-119.

10. The Battle of the Atlantic

1 Peter Padfield, *Dönitz: The Last Führer, Portrait of a Nazi War Leader*, Victor Gollancz, London, 1984, p. 206.

11. Classical Enemies, Modern Codebreaking

1 From 'Greek Military Intelligence and the Italian Threat, 1934–1940', *Journal of Intelligence History*, quoted on Christos' Military and Intelligence Corner, 24 October 2017, 'Signals Intelligence and Codebreaking Operations During the Greek–Italian War of 1940–41'.
2 Ibid. This explanation comes both from the above-mentioned, highly authoritative blog, and from TICOM, so it is possible that both have provided the same information from drawing the same deductions.
3 Walter Fricke's diary, and observations made about the Lauf monitoring station, appeared after the war as *War Secrets in the Ether*. The Italian material is in Volume 3, p. 25. Parts of the book have only just been declassified in Germany.

13. Losing Enigma

1 An SIS memorandum from 'C', the head of SIS, as quoted in *The Records of the Permanent Under-Secretary's Department, Liaison between the Foreign Office and British Secret Intelligence, 1873–1939*, p. 66, written by FCO historians Gill Bennett and Christopher Baxter, March 2005.
2 Jürgen Rohwer and Eberhard Jakel (eds), *Die Funkaufklärung und ihre Rolle im Zweiten Weltkrieg* (trans. Signals Intelligence and its Role in the Second World War), Stuttgart, 1979, p. 386.
3 TICOM DF I-12: *The Preliminary Interview with Wilhelm Tranow*, on 24–26 May 1945 at Flensburg.

14. The Good Colonel

1 *Intercepted Communications for Field-Marshal Erwin Rommel,* historynet.com, 30 March 2008, by Will Deac, p.1.
2 TICOM DF-116 Y, which is a transcript of Army Security Agency report AS-14, in which Fricke details the breaking of the United States' military attaché's codes.
3 Ibid.
4 Ibid.
5 Ibid.
6 TICOM DF-116-Z: *The Fellers Code Supplement.*

7 TICOM DF-187B: *The Organization of OKW-Chi.*
8 historynet.com, as in note 1 above.
9 Signal from Bonner Fellers to the US Military Intelligence Division, 1 February 1942, US Military Attaché, Cairo, Records of the War Department General and Special Staffs, Records Group 165, NARA (National Archives).
10 C. J. Jenner, 'Turning the Hinge of Fate: Good Source and the UK–US Intelligence Alliance, 1940–1942', *Diplomatic History*, Volume 32, Issue 2, 1 April 2008, pp. 165–205, this is from p. 176, in turn quoting 'The Contribution of the Information Service to the May–June 1942 Offensive in North Africa', File 1035, Records Group 457, NARA, Maryland, US.
11 C. J. Jenner, 'Turning the Hinge of Fate', p. 185, citing Memorandum from Chief of Staff for the President, 23 June 1942, Records Group 218, NARA, Mayland, US.

15. Signals Intelligence and Cryptanalysis on the Russian Front

1 TICOM document DF-112: *Survey of Russian Military Systems*, pp. 1–111. This is almost entirely based on lengthy interviews with Lieutenant Alexis Dettmann, who was the officer in charge of the Russian section of the signals intelligence agency of the GdNA. The information about his activities before and during the war come from this TICOM document, and were written by Dettmann over several months in 1947 and received by the US Army Security Agency. Dettmann was in British captivity from January to May 1945, and placed himself at the disposition of the Americans in 1947.
2 TICOM DF-112.
3 TICOM DF-112, p. 107.
4 TICOM IF-178: *The Seabourne Report Volume II, Part 1: Biographies of Personnel from the Luftwaffe's Signals Intelligence Service*, p. 1, Colonel Hans Eick. His continuing story before and during Operation *Barbarossa* is drawn from this dossier.
5 Extracted from TICOM DF-112.
6 Major Lonnie O. Ratley III, March–April 1983, *A Lesson of History: The Luftwaffe and Barbarossa*, Air University Review, Maxwell US Air Force Base, USAF Air Educational and Training Command, Montgomery, Alabama.
7 TICOM I-12: *Interview with Wilhelm Tranow*.
8 Ibid.
9 TICOM DF-18, pp. 58–62.
10 TICOM I-173 p. 6.
11 TICOM I-79, p. 8.
12 DF-112: *Survey of Russian Military Systems*.

13 Ibid., pp. 110–12.
14 Stephen G. Fritz, *Frontsoldaten: The German Soldier in World War II*, University Press of Kentucky, Kentucky, 1997, pp.105 and 114.
15 Allen F. Chew, *Fighting the Russians in Winter: Three Case Studies*, Leavenworth Papers, Combat Studies Institute, US Army Command and General Staff College, Fort Leavenworth, Kansas, December 1981.
16 Stephen G. Fritz, *Frontsoldaten*, pp. 105 and 114.
17 TICOM DF-111: *Comments on various cryptologic matters by Adolf Paschke*.
18 TICOM IF-178: *The Seabourne Report Volume 2, Part 1, The Signials Intelligence Service of the Luftwaffe, Biographies of Contributors: Captain Wadim Herold*, pp. 14–21.
19 Christer Bergström, *Stalingrad – The Air Battle: 1942 through January 1943*, Midland Publishing, Hinkley, UK, 2007, p.43.
20 *Duelling Aces in Sevastopol*, by Christer Bergstrom and Andrey Mikhailov, Warfare History Network, 4 November 2017.
21 ' *The Battle of Stalingrad. Signal Communications in the Pocket of Stalingrad and Communications with the Outside*', General-Major Wilhelm Arnold; US Army, Europe 1952–1954, Historical Division. Foreign Military Studies Branch. Foreign Military Studies D-271 published 1947. All the quotes about the Battle of Stalingrad in Chapter 15 come from this same source.
22 TICOM DF-112.

16. The Enigmatic Swiss

1 TICOM I-193: *Interview with SS-Obersturmbannführer Urban*, Liaison Officer between the RSHA and Hungarian Military Intelligence.
2 These are all headlines from wartime newspapers held in the archives of the American Red Cross.
3 'The ICRC in WWII – The Holocaust', 24 January 2014; the article appears on the website of the International Committee of the Red Cross, www.icrc.org.
4 '*European Axis Signal Intelligence in World War II*', Volume 1, May 1946 in 'Results of European Axis Cryptanalysis' – Switzerland.
5 US State Department Report February 1946, p. 31, '*Achievements of the Signal Security Agency in World War II*'.
6 TICOM I-45: *OKW/Chi Cryptanalytic research on Enigma, Hagelin and Cipher Teleprinter machines*.
7 Ibid.
8 Pers-Z file 'Bericht der Belgisch-Französisch-Schweizerischen Gruppe Stand 1.12.1941'.
9 TICOM DF-240A: *Characteristics, Analysis and Security of Cryptanalytical Systems,*

written in April 1951 by three contributors, former members of the Forschungsamt, including Dr Bruno Kroeger; also from TICOM DF-241: *The Forschungsamt – Part IV.*

10 TICOM DF-240 / 241; also from *The compromise of the Swiss diplomatic Enigma K cipher machine in WWII,* Christos' Military Intelligence Corner, 1 October 2017.

17. Rhubarb and Rodeo

1 Terry Copp, 'The Air over Dieppe', *Legion*, June 1996, p. 8.

2 Ronald Atkin, *Dieppe 1942: The Jubilee Disaster*, Book Club Associates, London, 1980, p. 264.

18. U-91 and the Battle of the Atlantic

1 Terry Hughes and John Costello, *The Battle of the Atlantic*, Dial Press / J.Wade, New York, 1977, p.6. Also quoted in David Kahn, *Codebreaking and the Battle of the Atlantic*, 4 April1994, The USAFA Harmon Memorial Lecture No. 6, p. 1.

2 uboat.net

3 BdU War Diary 3–9 September 1942, 79/446, Volume 6, Chapter 10, Operational Archives Branch, Naval Historical Center, Washington, DC.

4 *U-Boat Attack Logs; A Complete Record of Warship Sinkings from Original Sources 1939–1945*, Daniel Morgan and Bruce Taylor (Forward by Jürgen Rohwer), Seaforth Publishing / Pen & Sword Books, Barnsley, UK, 2011. The entire attack sequence of U-91 on HMCS Ottawa, from 0150 to 0215 on the 14th (German Time) is reproduced on page xxv of the Introduction. This authoritative volume in turn draws on most of the main original repositories of sources for U-boat sinkings, including The Naval Historical Center in Washington, DC; The Royal Naval Museum, Portsmouth, UK; Deutsches U-Boot Museum-Archiv in Cuxhaven-Altenbruch, Lower Saxony, Germany; The Sammlung Rohwer (the collection of archive material accumulated by Jürgen Rohwer); The Naval Historical Branch of the British Ministry of Defence in Portsmouth, UK; and The Bundesarchiv in both Freiburg and Koblenz, Germany.

5 The first sighting of Convoy ON 127 was made from the surface – from where U-91 attacked.

6 Walkerling's attack log is written in German Time, which he records then as being two hours ahead of Allied Time, so for him, the attack took place on the 14th, for the Allies, the 13th.

7 Taken from the log of U-91 for 12–14 September 1942, written by Heinz Walkerling. Quoted in *U-Boat Attack Logs.*

8 The number of U-boats in the three combined wolfpacks varies across the main sources, both the museum and archive material named above, and on uboat.net and convoyweb. org. The variance is from thirty-seven to forty-five. While as many as forty-five actual U-boats probably participated in all the attacks, some of these were not actually from the three wolfpacks, but were either sailing independently or had been ordered to join in the attack from as far away as the Caribbean.

9 The complement of U-91 on its patrols varied between forty-four and sixty.

10 *Life Aboard a U-Boat,* from uboataces.com, and *The food onboard the U-Boats,* from uboat. net, which details the assessment of provisions carried aboard a Type IXC U-Boat for a three-month patrol.

11 The sourcing of the total number of merchant ships and escorts that sailed with or alongside both Convoys HX-229 and SC-122 gives a variation, as some escorts were only with the convoys for one to four days, and some merchant vessels detached themselves with technical difficulties. Arnold Hague's highly authoritative convoyweb.org is a clear and accurate source. Jürgen Rohwer's account of the convoy battle fills all of his book, *The Critical Convoy Battles of March 1943: The Battle for HX 229/SC 122*, Naval Institute Press, Annapolis, 1977.

12 Martin Middlebrook, *Convoy,* Viking Press, New York, 1976, p. 276. The phrase was broadcast on German radio.

13 www.ibiblio.org, in its *Battle of the Atlantic III: German Naval Communications Intelligence (SRH-024), Chapter IV, Compromise of Naval Ciphers 3 and 5 (Anglo-US)* details the signals compromise very clearly and vividly. This draws on documentation from the NSA's Central Security Agency.

19. The Battle of the Aegean

1 TICOM I-203: *Interrogation of Herbert Marinick and Herbert Korn, Former Members of the Reichpost and OKW/Chi*.

2 *The London Gazette* (Supplement), 8 October 1948.

20. Insecure Enigma

1 US Army Security Agency WDGAS-14: *European Axis Signal Intelligence in World War Two*, Volume 3, the Signal Intelligence Agency of the Armed Forces, High Command, US Army Security Agency, 1st May 1946.

2 Ibid., WDGAS-14.

3 An analysis and summary of the plan was made by the American National Security Agency in 1947, by Joseph A. Meyer, NSA Document ID 3838699, *Der Fall Wicher: German Knowledge of Polish Success on Enigma.* Quotations used are from pp. 1–17. Additional details on Case Wicher are drawn from TICOM interviews with Dr Otto Buggisch from OKW-Chi, the mathematician who led some of the investigations into it: these appear in TICOM-I-58, an interview with Otto Buggisch carried out on 8 August 1945, and from TICOM I-46: *Preliminary Report on Interrogation of Dr. Otto Buggisch (of OKH/Gen.d.NA) and Dr. Werner Liebknecht,* 23 June 1945. Additional details appear in TICOM I-46, 64, 66, 67 and 137.

4 Joseph A. Meyer, *Der Fall Wicher*, p. 2.

5 Friedrich L. Bauer, *Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie* (trans. Decrypted Secrets – Methods and Maxims of Cryptography) (third edn), Springer, Heidelberg, 2000; TICOM I-39: *Organisation of OKW-Chi*.

6 Extracted from the War Diary of the Oberkommando des Heeres, or OKH, quoted in Joseph A. Meyer, *Der Fall Wicher*, p. 10.

7 TICOM IF-189: *Preliminary Interrogation of Friedrich Stohlket.* This was done in November 1945 – the subject was a former member of the Heer Signals Corps who worked on decrypting Russian codes.

21. The Coming Storm

1 Charles Fenyvesi, *Washington Post*, 26 May 1998, 'Japan's Unwitting D-Day Spy'.

2 TICOM I-143: *Report on the Interrogation of Five Leading Germans at Nuremberg on 27 September 1945*.

3 *The Cicero Papers,* March 1 2005, FCO Historians.

4 TICOM I-109.

5 Lieutenant Martin Ludwig's interview by TICOM on US and British air force codes appears in TICOM I-109.

22. Execution and Capture

1 Francis Harry Hinsley et al., *British Intelligence in the Second World War,* 5 Volumes, HMSO, London, 1979–1988.

2 B. Jack Copeland, *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford University Press, Oxford, 2010, pp. 1–6.

3 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in*

Europe and the West, Penguin Books, London, 2000, p. 150, note 13.

4 Joseph A. Meyer, *Der Fall Wicher*.

23. The Collapse of the Third Reich

1 TICOM IF-179 *The Seabourne Report Volume IV Part 2: Biography of Major Ferdinand Feichtner CO 352nf Regt South SIS German Luftwaffe*.

2 Ibid.

3 Ibid.

4 Cyril E. Black, Robert D. English, Jonathan E. Helmreich and James A. McAdams, *Rebirth: A Political History of Europe Since World War II*, Westview Press, 2000, p. 61.

5 TICOM I-193: *Interview with SS-Obersturmbannführer Urban,* Liaison Officer between the RSHA and Hungarian Military Intelligence.

6 In the TICOM report, DF-112, in which this appears, the second half of the quote is written in English.

7 TICOM DF-112, p. 109, *Interview with Leutnant Alexis Dettmann*.

8 TICOM IF-179: *The Seabourne Report Volume IV Part 2: Biography of Major Ferdinand Feichtner CO 352nf Regt South SIS German Luftwaffe*.

9 TICOM IF-178: *The Seabourne Report Volume II: Biographies of Personnel from the Luftwaffe's Signals Intelligence Service*.

10 TICOM DF-187: *The Career of Wilhelm Fenner with Special Regard to His Activity in the Field of Cryptography and Cryptanalysis.*

11 Glenn B. Infield, *Skorzeny: Hitler's Commando*, St Martin's, New York, 1981, pp. 22–3.

24. The Man with the Key has Gone

1 TICOM document NN/ 37/5847, *Narrative and Report of Proceedings of TICOM Team 6*, 11 April–6 July 1945, written by Commander A.M.S. Mackenzie, Royal Navy Volunteer Reserve.

2 Ibid.

3 TICOM I-12: *A Translation of the Preliminary Interrogation of Oberregierungsrat (Senior Civil Service Administrator) Wilhelm Tranow of 4SKL / III of OKM*, carried out at Flensburg on 24/25 May by TICOM Team 6, pp. 1–15.

Conclusion

1 Evaluation of the Role of Decryption Intelligence in the Operational Phase of the

Battle of the Atlantic, Department of the Navy, Office of the Chief of Naval Operations, Operations Evaluation Group, Report 68 Reference A/65650 / (LO) 2271-52, pp. 5, 9 and 18. The report itself is undated, but the copy quoted here is one sent from the OEG's Director, Jacinto Steinhardt, to the Vice-Director of the National Security Agency, Rear-Admiral Wenger, on 1 April 1953.

2 *Codebreaking and the Battle of the Atlantic*, USAFA Harmon Memorial Lecture 6, David Kahn, 4 April 1994, p. 7.

3 Review of Security of Naval Codes and Cyphers 1939–1945, by Paymaster Commander W. G. S Tighe, RN, British Public Records Office, Kew, UK, DM 1/27186. As the information closely reflects that which Wilhelm Tranow gave in his interviews with TICOM teams, it seems reasonable to deduce that it is partly based on them. The US Navy's Operations Evaluation Group Report 68, referenced above, says however that the German B-Dienst supplied U-Boat headquarters with what it calls 'good intelligence' on Allied convoys for 37% of the time between July and December 1942, and for 72% of the time between January and May 1943.

4 *Ultra and the Battle of the Atlantic: the German View,* Naval Symposium at the US Naval Academy, Annapolis, Maryland, 28 October 1977.

ACKNOWLEDGEMENTS

For different kinds of help, guidance and wisdom during the writing of this book, thanks must go to Cordula Kraemer in Berlin, to Giulia Avataneo, Daniele Calafiore, Otilia Cheslerean and Amor Ben in Turin, and to my brother Martin in Oxford. Laura Callaghan and Gemma Gardner at Osprey Publishing have helped enormously with this and two of my other books.

OSPREY PUBLISHING
Bloomsbury Publishing Plc
PO Box 883, Oxford, OX1 9PL, UK
1385 Broadway, 5th Floor, New York, NY 10018, USA
E-mail: info@ospreypublishing.com
www.ospreypublishing.com

This electronic edition published in 2018 by Bloomsbury Publishing Plc

OSPREY is a trademark of Osprey Publishing Ltd

First published in Great Britain in 2018

© Christian Jennings, 2018

Christian Jennings has asserted his right under the Copyright, Designs and Patents Act, 1988, to be identified as Author of this work.

For legal purposes the Acknowledgements constitute an extension of this copyright page.

All rights reserved
You may not copy, distribute, transmit, reproduce or otherwise make available this publication (or any part of it) in any form, or by any means (including without limitation electronic, digital, optical, mechanical, photocopying, printing, recording or otherwise), without the prior written permission of the publisher. Any person who does any unauthorised act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

A catalogue record for this book is available from the British Library.

ISBN: 978-1-4728-2950-4 (HB)
ISBN: 978-1-4728-2954-2 (PB)
ISBN: 978-1-4728-2951-1 (eBook)
ISBN: 978-1-4728-2952-8 (ePDF)
ISBN: 978-1-4728-2953-5 (XML)

Editor's note
For ease of comparison please refer to the following conversion table:
1 mile = 1.6km
1yd = 0.9m

1ft = 0.3m
1in = 2.54cm/25.4mm
1 gallon = 3.8 litres
1lb = 0.45kg

Osprey Publishing supports the Woodland Trust, the UK's leading woodland conservation charity. Between 2014 and 2018 our donations are being spent on their Centenary Woods project in the UK.

To find out more about our authors and books visit **www.ospreypublishing.com**. Here you will find our full range of publications, as well as exclusive online content, details of forthcoming events and the option to sign up for our newsletters. You can also sign up for Osprey membership, which entitles you to a discount on purchases made through the Osprey site and access to our extensive online image archive.

Содержание

Cover 1
Title Page 3
Contents 5
Preface 7
Part One: Germany Ascendant 18
1. Losing the Signals Intelligence Battle in World War I 19
2. The Enigma Salesman 39
3. Germany’s New Codebreakers 55
4. Preparing for War 64
5. The Kriegsmarine Starts Listening 80
Part Two: Germany Offensive 92
6. Two Navies at the Outbreak of War 93
7. Romanian Codes and Romanian Oil 108
8. Signals and Deception in the Invasion of Europe 115
9. Fighting the War in the Air 125
10. The Battle of the Atlantic 134
11. Classical Enemies, Modern Codebreaking 145
Part Three: Germany at War 152
12. Germany’s Mediterranean Battles 153
13. Losing Enigma 162
14. The Good Colonel 172
15. Signals Intelligence and Cryptanalysis on the Russian Front 183
16. The Enigmatic Swiss 210
17. Rhubarb and Rodeo 217
18. U-91 and the Battle of the Atlantic 222
Part Four: Germany Defensive 238
19. The Battle of the Aegean 239
20. Insecure Enigma 252
21. The Coming Storm 262
22. Execution and Capture 276

23. The Collapse of the Third Reich 285
24. The Man with the Key has Gone 293
Epilogue: What Became of the Characters after the War? 303
Conclusion 307
Photographs 315
Chronology 349
Bibliography and Sourcing 356
Glossary 359
Endnotes 362
Acknowledgments 374
eCopyright 375